NTP Software File Auditor

User Manual

June 2012

This manual details the method for using NTP Software File Auditor, from an administrator's perspective. Upon completion of the steps within this document, NTP Software File Auditor will be used to monitor file and directory operations for users within your enterprise community.

Table of Contents

Executive Summary 4

NTP Software File Auditor Configuration 5

Setting NTP Software File Auditor Properties 6

- Setting the NTP Software File Auditor Security Level 6
- Setting the NTP Software File Auditor Database 7
- Setting the NTP Software File Auditor Email 10
- Setting the NTP Software File Auditor Miscellaneous Options 11

Policy Creation 12

- Creating File Audit Policies 13
- Viewing Directories 21
- Viewing Shares 22

NTP Software File Auditor Reports 23

Retrieving Records Archived via ODDM 38

File Auditor Business Overwatch Tasks (BOTs) 42

Defining or Editing a BOT 42

Default BOTs 50

File Auditor Database and Email Settings 51

- Database Settings 51
- Email Configuration 52

File Auditor BOTs Demo Mode 53

NTP Software Smart Policy Manager 54

- NTP Software Smart Policy Manager Overview 54
- Managing the NTP Software File Auditor Service through an NTP Software File Auditor Admin Client Running on a Different Machine 55
- Installing the NTP Software Smart Policy Manager Admin Component 56
- Installing the NTP Software File Auditor Admin Component 60
- Administering NTP Software File Auditor through an NTP Software File Auditor Admin Client Running on a Different Machine. 67

Installing File Auditor in Clustered Environments 68

- Installing the NTP Software File Auditor in Clustered Environments 69

Copyright © 2012 by NTP Software®. All rights reserved.

Installing the NTP Software File Auditor onto a Node Server 72
Network Attached Storage (NAS) Preparations 74
Preparing the NetApp Filer 74
Enabling the fpolicy Management Service (NetApp Filers) 74
Adding Your Filer to the NTP Software File Auditor Policy Hierarchy 76
Preparing the EMC Celerra 77
Preparing EMC Celerra to be managed by File Auditor 77
Preparing File Auditor Windows Machine – Scenario A 77
Adding a Celerra to the NTP Software File Auditor Policy Hierarchy 81
Preparing File Auditor Windows Machine – Scenario B 82
Preparing the BlueArc Titan or Hitachi NAS 87
Preparing the BlueArc Titan/ Hitachi NAS for NTP Software File Auditor Management 87
Adding an EVS to the NTP Software File Auditor Policy Hierarchy 88
About NTP Software 89
NTP Software Professional Services 89

Copyright © 2012 by NTP Software®. All rights reserved.

Executive Summary

Thank you for your interest in NTP Software File Auditor™. NTP Software File Auditor extends our best-of-breed technology, allowing you to manage NAS-hosted storage as a seamless whole.

NTP Software File Auditor lets you monitor your users' file and directory operations. It lets you create and enforce file audit policies that enable you to monitor certain events taking place in your environment. Such events include directories created, renamed, and/or deleted and files opened for read, write, create, rename, delete, and/or close in your environment.

NTP Software File Auditor has two main components:

1. NTP Software File Auditor Administrator
2. NTP Software File Auditor Reports

Each of the above components will be explained in further details in the next sections.

Please refer to the Network Attached Storage (NAS) Preparations section before you start working with NTP Software File Auditor.

Given the architecture of your NetApp® Filer®, EMC®Celerra®, BlueArc® Titan, or Hitachi NAS, NTP Software File Auditor does its job remotely. NTP Software File Auditor uses a connector service to create a bridge and include Filers/Celerras/Titans/Hitachi NASs as full participants in storage environments audited by NTP Software File Auditor. In light of this fact, you will need to install the NAS/EMC/BlueArc/Hitachi connector on one of the Windows® 2000, Windows Server® 2003, or Windows Server® 2008 machines in your environment. This can be an existing server or workstation, or a standalone system.

To be audited by NTP Software File Auditor, version 6.5 or later (excluding version 7.1) of the Data ONTAP® operating system for Filers, or version 5.6.36.2 or later of the DART® operating system for Celerras, or version 6.1.1684.18 of the BOS operating system for Titans, or version 6.1.1684.18 of the NOS operation system for Hitachi NASs is required. NTP Software File Auditor can be used to audit Filers, Celerras, Titans, Hitachi NASs, Filer clusters, Celerra clusters, Titan clusters, and Hitachi NAS clusters; or any combination of these systems. NTP Software File Auditor imposes no restrictions on how you monitor your file and directory operations. You can impose policies on individual files, directories, users, and/or groups of users.

To install NTP Software File Auditor a login with administrator rights is needed. You will be installing three different services: the NTP Software Smart Policy Manager™ service, the NTP Software File Auditor service, and the NAS/BlueArc/Hitachi connector service.

Your hardware should be appropriate for the services running on each machine.

Copyright © 2012 by NTP Software®. All rights reserved.

NTP Software File Auditor Configuration

The NTP Software File Auditor Configuration Wizard appears once the NTP File Auditor installation completes. It enables you easily to add the Filer, Celerra, or EVS to be monitored by the NTP Software File Auditor application. To use the NTP Software File Auditor Configuration Wizard, please follow these steps:

1. Click **Start** > **Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor™ for NAS Configuration Wizard**.
2. Click the **View Pre-Wizard Checklist** button and gather the required information before continuing. Click **Next**.
3. Enter the name of your Filer, Celerra, or EVS. Click **Finish**.

Copyright © 2012 by NTP Software®. All rights reserved.

Setting NTP Software File Auditor Properties

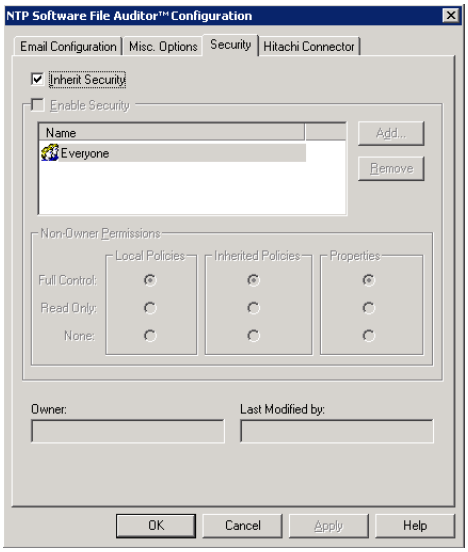
NOTE: For all the screens displayed in this user manual, an NTP Software File Auditor for NAS NetApp/IBM N Series edition is used. Please note that screenshots differ depending on the NTP Software File Auditor edition being installed.

Setting the NTP Software File Auditor Security Level

The NTP Software File Auditor Properties tab enables you to set up several application properties, including the application security level. To adjust your NTP Software File Auditor application security level, please follow these steps:

1. On the left tree view, expand the MySite node.
2. Right-click **NTP Software File Auditor** under MySite navigate to the Windows server node and select **Properties** from the Menu.
3. Click the **Security** tab. Clear the **Inherit Security** box and check the **Enable Security** checkbox. Click **Add** to choose the users or groups for which you want to apply security options.

Tip: In the **Non-Owner Permissions** section of the dialog box, choose the desired settings for the types of policies and properties.



4. Click the **NAS/EMC/BlueArc/Hitachi Connector** tab to add/remove the NetApp/EMC/Titan(s)/Hitachi NAS(es) to be managed.

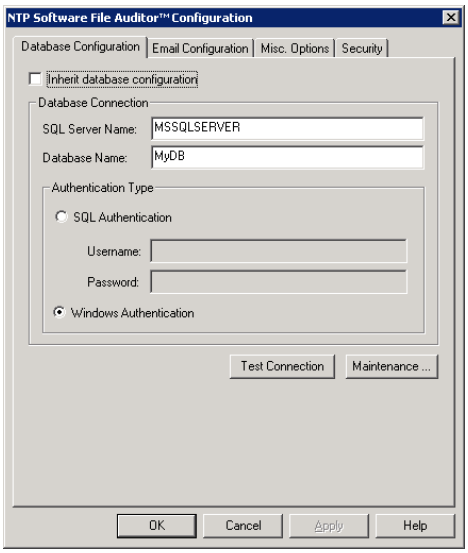
Copyright © 2012 by NTP Software®. All rights reserved.

Setting the NTP Software File Auditor Database

The NTP Software File Auditor Properties tab enables you to set up several application properties, including the application database. Your application database configuration should be adjusted before creating any file audit policies, because all of the events monitored through the File Auditor policies are saved to your configured database. To configure the database, please follow these steps:

1. Right-click **NTP Software File Auditor** under the main application container (**My Organization**, in this example).
2. Right-click **NTP Software File Auditor** under Organization Node and select **Properties** from the Menu.
3. On the **Database Configuration** tab, clear the **Inherit Database Configuration** box, enter the correct information in each of the text boxes as appropriate for your database, and click **OK**.

> **NOTE:** "My Organization" is the main application container, so the database configuration specified here is inherited by any other server created within the tree. This saves the administrators from having to enter the database configuration manually.

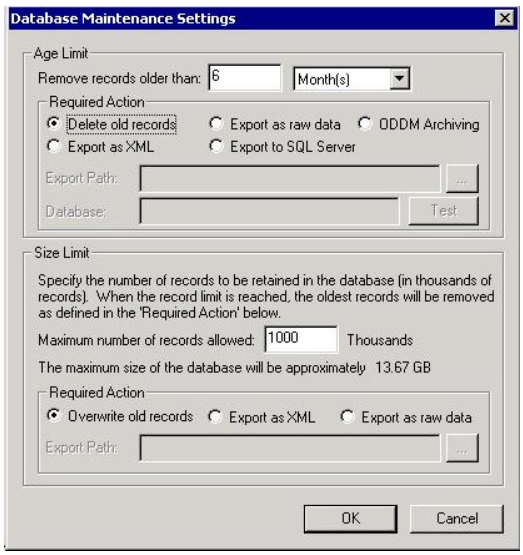


4. If you want to specify different database configurations, right-click **File Auditor** under the NetApp Filer/EMC Celerra/BlueArc Titan/ Hitachi NAS that has been added.

Copyright © 2012 by NTP Software®. All rights reserved.

5. If you want to back up/delete old files to maintain the size of your database, click the **Maintenance** button.

> **NOTE:** The DB Maintenance option works on two levels, the server level and the policy level.



On the **Database Maintenance Settings** dialog, under the **Age Limit** section use the **Remove records older than** field to set the number of days/weeks/months/years File Auditor should keep records in the primary database, after which File Auditor will attempt to back them up.

Based on the **Required Action** field; File Auditor can delete old records from the database, export old records to a comma-separated file, export aging records to an XML file, export aging records to a database you specify on the SQL server instance you specify, or use On-Demand Data Movement (ODDM) to back-up old records.

File Auditor Reports retrieve old records for reporting purposes. You can configure File Auditor to use your On-Demand Data Movement (ODDM) by setting two fields, those are:

- The temp. share, which is a temporary share on your primary server that ODDM uses as a source for files to back-up. The Service account for File Auditor services must have *Read, Write and Delete* permissions on this share. For information about ODDM Primary Servers, please refer to the *NTP Software ODDM™ Administration Web Site - User Manual.*
- The Web Service, which is a URL to the ODDM Web Service.
  (e.g. http://BackupHost/ODDMAdmin/ODDMService.asmx)

Copyright © 2012 by NTP Software®. All rights reserved.

Please refer to the Retrieving Records Archived via ODDM section for more details on how to use File Auditor Reports to retrieve your old records archived via ODDM in order to run reports on them.

NOTE: File Auditor reports will retrieve records only if the records are archived using On-Demand Data Movement (ODDM).

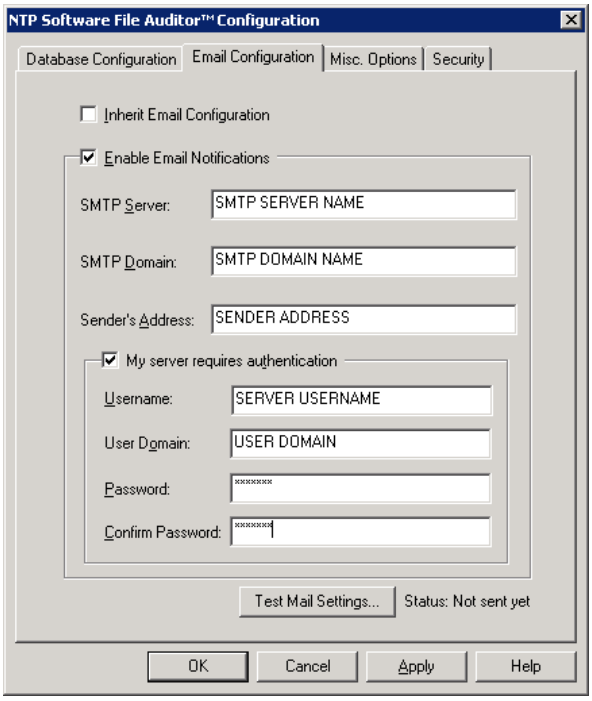
Copyright © 2012 by NTP Software®. All rights reserved.

Setting the NTP Software File Auditor Email

The NTP Software File Auditor Properties tab enables you to set up several application properties, including the application emails. To adjust your NTP Software File Auditor application email feature, please follow these steps:

1. Right-click **NTP Software File Auditor** under the main application container.
2. Click **Properties** on the pop-up menu.
3. Click the **Email Configuration** tab. Clear the **Inherit Email Configuration** box. Check the **Enable Email Notifications** option. Enter the correct information in each of the text boxes as appropriate for your email settings, and click **OK**.

> **Tip:** Click the **Test Mail Settings** button to test your connection to the specified SMTP Sever. Specify the email ID to which the test email should be sent. If the email is sent successfully, the status field will display Test mail sent. Otherwise, it will display Test mail not sent.

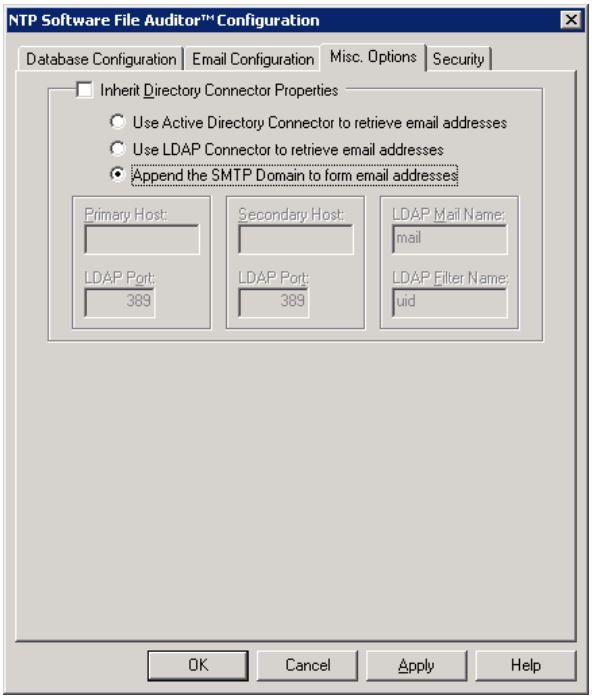


Copyright © 2012 by NTP Software®. All rights reserved.

Setting the NTP Software File Auditor Miscellaneous Options

The NTP Software File Auditor Properties tab enables you to set up several application properties, including the application miscellaneous options. To adjust your NTP Software File Auditor application miscellaneous options, please follow these steps:

1. Right-click **NTP Software File Auditor** under the main application container.
2. Click **Properties** on the pop-up menu.
3. Click the **Misc Options** tab. Clear the **Inherit Directory Connector Properties** box and select the appropriate directory connector option.



Copyright © 2012 by NTP Software®. All rights reserved.

Policy Creation

This section outlines standard NTP Software File Auditor procedures for creating a File Auditor policy.

NOTES:

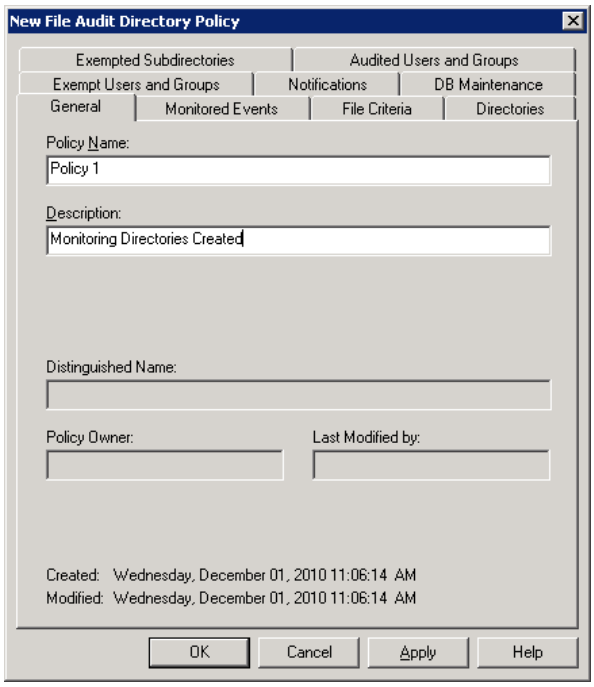
- NTP Software File Auditor monitors two main types of paths: **directory paths** and **share paths**. For share paths, all you need to do is add a share name. For directory paths, the format depends on the NTP Software File Auditor edition being used:
  - For NAS NetApp edition, the directory path format is \vol\<*volume name*>\<*some directory*>[…*optional subdirectory**another optional subdirectory*].
  - For NAS EMC, the directory path format is \<file system mount path>\<*some directory*>[…*optional subdirectory**another optional subdirectory*].
  - For BlueArc or Hitachi editions, the directory path format is \fs\<*volume name*>\<*some directory*>[…*optional subdirectory**another optional subdirectory*].
- When testing policies you have created, perform the tests from an independent machine that is *not* running NTP Software File Auditor.

Copyright © 2012 by NTP Software®. All rights reserved.

Creating File Audit Policies

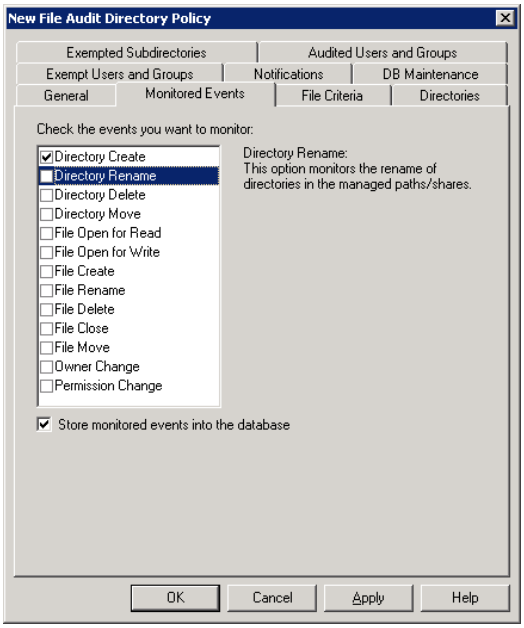
This section walks you through creating a typical file audit policy. We will create a file audit policy for all your user home directories in a typical server configuration. This policy will be applied to all users in your Users directory.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the Filer/Celerra/EVS you added earlier. If necessary, click the plus sign (**+**) adjacent to this entry to expand the tree. Then click the plus sign next to **File Auditor** to expand the policy types.
2. Right-click **File Audit Policies** and select **New** > **Folder Policy Using Directories**.
3. In the **New File Audit Directory Policy** dialog box, click the **General** tab. Enter a name and a description for your new policy.



Copyright © 2012 by NTP Software®. All rights reserved.

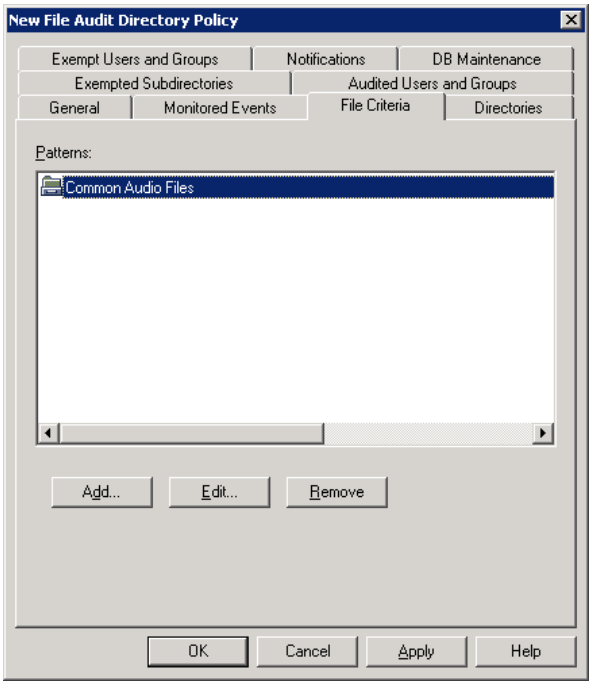
4. Click the **Monitored Events** tab; check the event(s) you want to monitor from the list of events. Check the **Store monitored events into the database** checkbox if you wish to store the monitored events in the File Auditor database. You can clear the **Store monitored events into the database** checkbox if you wish to use the notifications option without recording the events to the File Auditor database.



Copyright © 2012 by NTP Software®. All rights reserved.

5. Click the **File Criteria** tab. Click the **Add** button, select the files that you wish to monitor, and the associated patters will be displayed automatically; you can also specify a custom pattern. Examples of custom patterns are using *.* (to manage all files) and using *.rtf, *.doc (to manage all Word files).

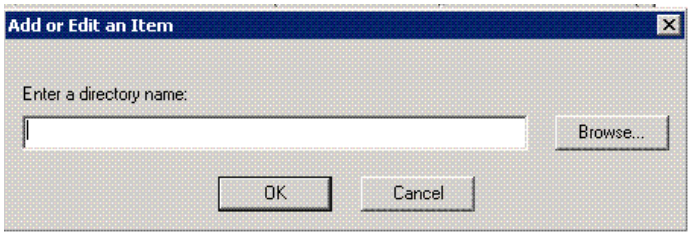
NOTE: If the Patterns list is empty, the policy will audit all of the file(s).



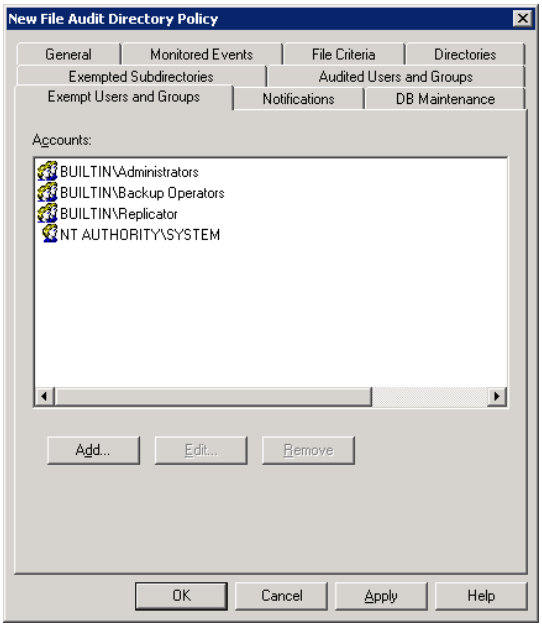
Copyright © 2012 by NTP Software®. All rights reserved.

6. Click the **Directories** tab. Click the **Add** button, type the appropriate directory path for your Users directory followed by a backslash.

> **NOTE:** By default, this policy applies to all users. You can verify this fact by clicking the **Managed Users and Groups** tab.

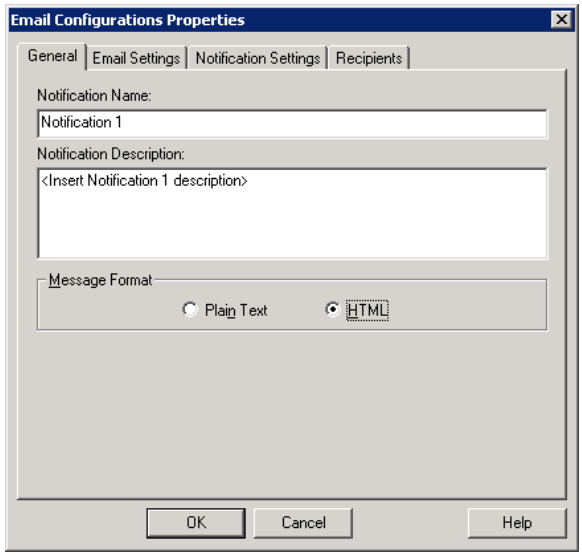


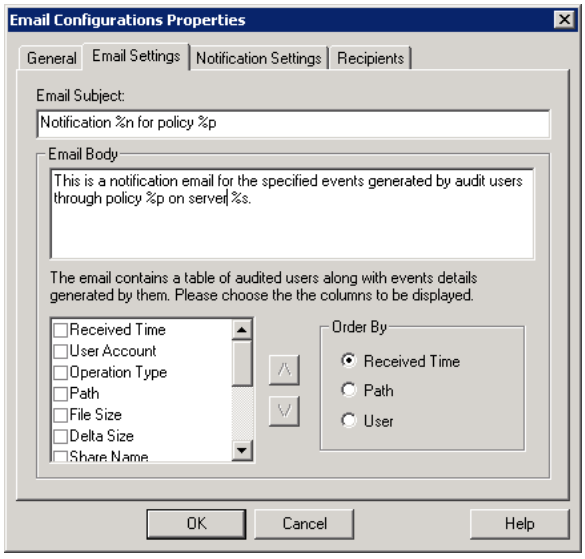
7. Usually administrators, backup operators, replicator, and the system account are exempt from policies. You can verify this fact by clicking the **Exempt Users and Groups** tab. To change this setting, select the appropriate entry and click **Remove**. To add an account click the **Add** button, browse and search for users/groups in Active Directory, select the user/group and click **OK**. The selected user/group will be added to the Exempt users list.



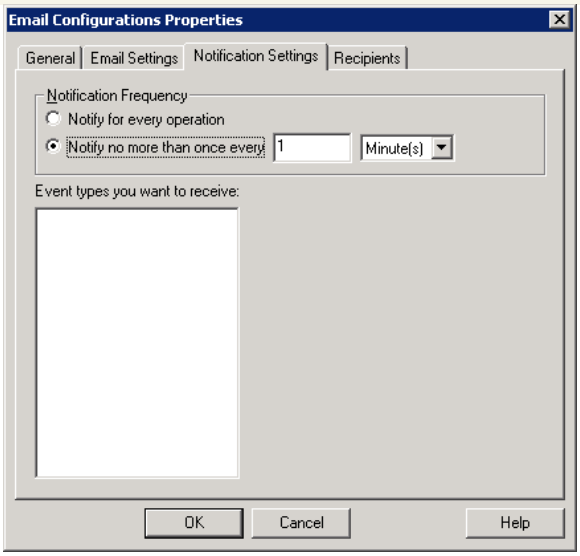
Copyright © 2012 by NTP Software®. All rights reserved.

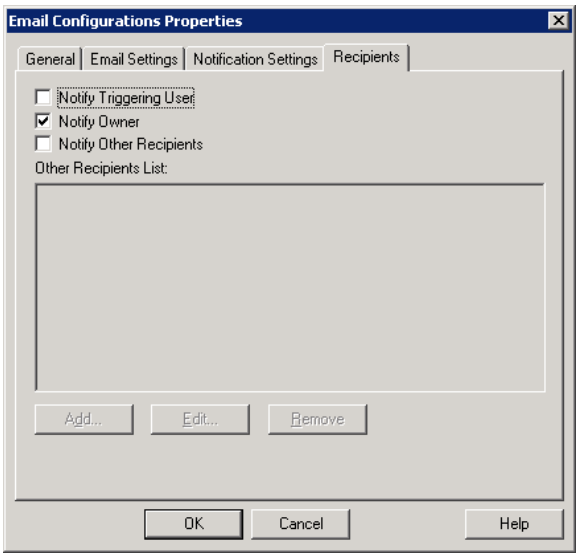
8. Click the **Notifications** tab, then click the **Add** button. On the **Email Configurations Properties dialog General** tab, specify the notification related details; including the notification name description and message format. On the **Email Settings** Tab, specify the email subject and the email body, customize the displayed information about the authorized users and the associating events, and choose the detail level. On the **Notification Settings** Tab, specify the notification frequency, along with the types of events you wish to receive. On the **Recipients** Tab, specify the user(s) who should receive the email.



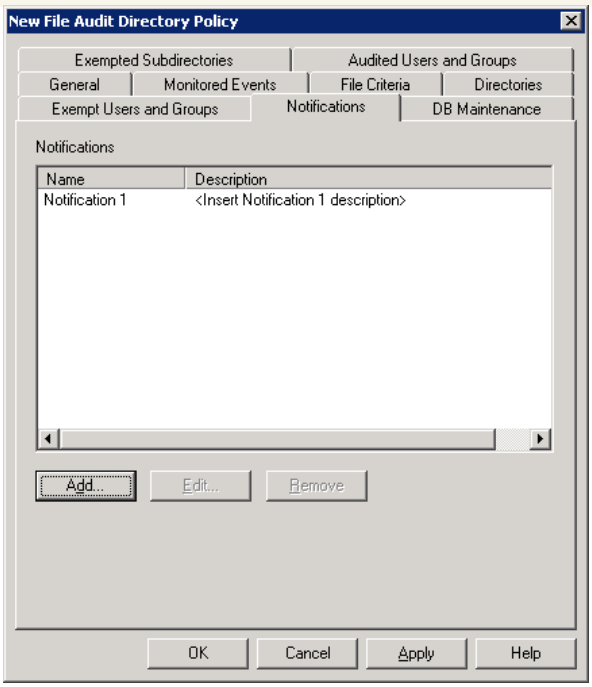


Copyright © 2012 by NTP Software®. All rights reserved.



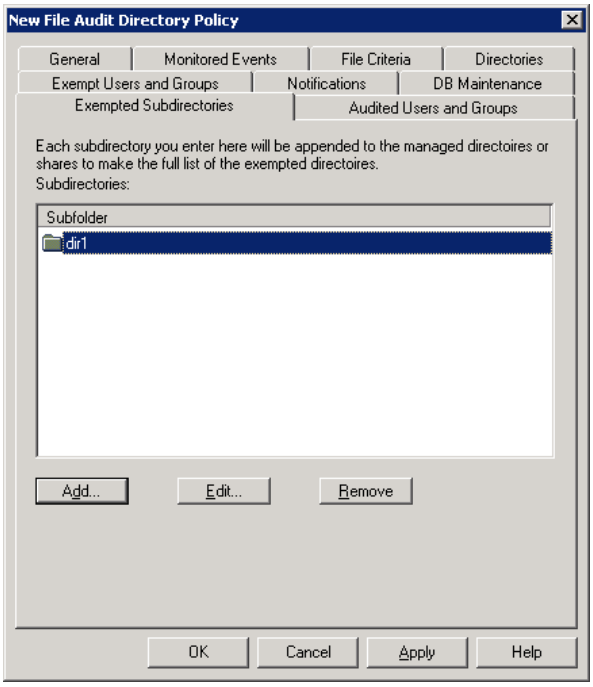


Copyright © 2012 by NTP Software®. All rights reserved.

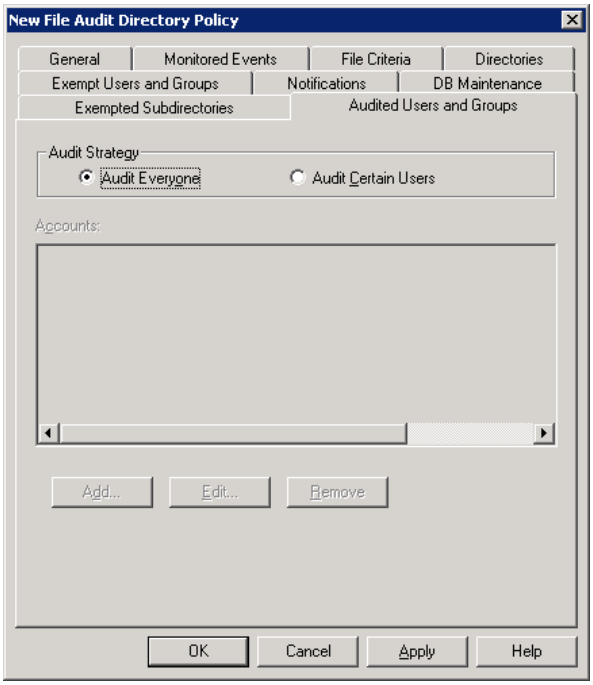


Copyright © 2012 by NTP Software®. All rights reserved.

9. Click the **Exempted Subdirectories** tab. Click the **Add** button and type the subdirectory you want to exempt from the monitored directories list.



10. Click the **Audited User and Groups** tab, choose whether you want to audit all users within your environment or specify certain user(s) to audit.



Copyright © 2012 by NTP Software®. All rights reserved.

11. Click **OK** to close the **New File Audit Directory Policy** dialog box. NTP Software File Auditor will create the new directory policy, which will be inherited by all systems from this point down in your hierarchy.

Viewing Directories

This section shows how you can view all the directories that are located on a certain Filer, Celerra, or EVS.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the Filer, Celerra, or EVS containing directories you want to view. If necessary, click the plus sign (**+**) adjacent to this entry to expand the tree.
2. Click the plus sign next to **File Auditor**.
   a. For the Filer, click the plus sign next to **Filer Directories** to view the volumes located on that Filer.

      NOTE: You can view that feature if you have a NetApp Filer attached to the NTP Software File Auditor application.

   b. For the Celerra, click the plus sign next to **Celerra Directories** to view the volumes located on that Celerra.

      NOTE: You can view that feature if you have an EMC Celerra attached to the NTP Software File Auditor application.

   c. For the EVS, click the plus sign next to **EVS Directories** to view the volumes located on the EVS.

      NOTE: You can view that feature if you have an EVS attached to the NTP Software File Auditor application.

Copyright © 2012 by NTP Software®. All rights reserved.

Viewing Shares

This section shows how you can view all the shared directories located on a certain Filer, Celerra, or EVS.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the Filer, Celerra, Titan, or Hitachi NAS with shared directories you want to view. If necessary, click the plus sign (**+**) adjacent to this entry to expand the tree.
2. Click the plus sign next to **File Auditor**.
    a. For the Filer, click the plus sign next to **Filer Shares** to view the volumes located on that Filer.

    > **NOTE:** You can view that feature if you have a NetApp Filer attached to the NTP Software File Auditor application.

    b. For the Celerra, click the plus sign next to **Celerra Shares** to view the shared folders located on that Celerra.

    > **NOTE:** You can view that feature if you have an EMC Celerra attached to NTP Software File Auditor application.

    c. For the EVS, click the plus sign next to EVS Shares to view the shared folders located on that EVS.

    > **NOTE:** You can view that feature if you have an EVS attached to NTP Software File Auditor application.

Copyright © 2012 by NTP Software®. All rights reserved.

NTP Software File Auditor Reports

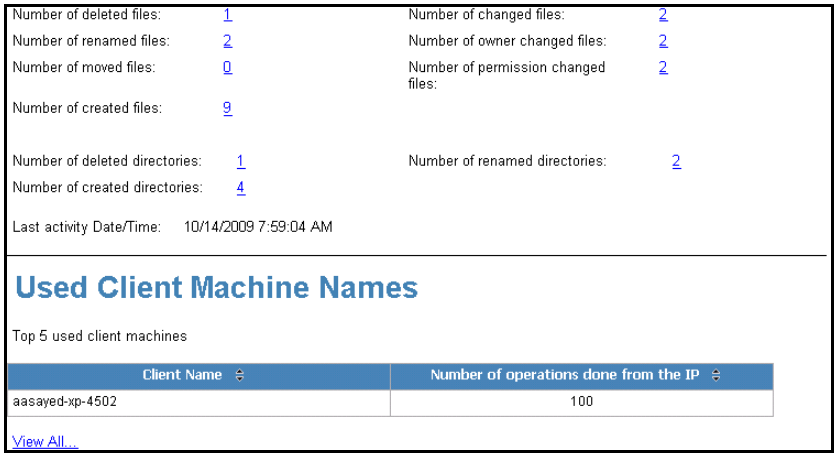
The NTP Software File Auditor reporting tool allows you to view the file and directory operations that took place at your environment in an easy and efficient display. Reports are categorized by user, file, policy, and folder.

To view NTP Software File Auditor Reports, please follow the following steps:

1. Run NTP Software File Auditor Administrator by clicking **Start** > **All Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor Reports**.
2. In the left pane, click the report type you want to display.
3. In the upper pane, specify the search criteria, then click **View Report**.
4. In the lower pane, check the report output.
5. NTP Software File Auditor also allows you to export the report to different formats. Those include XML, CSV, TIFF, PDF, Web Archive, or Excel.

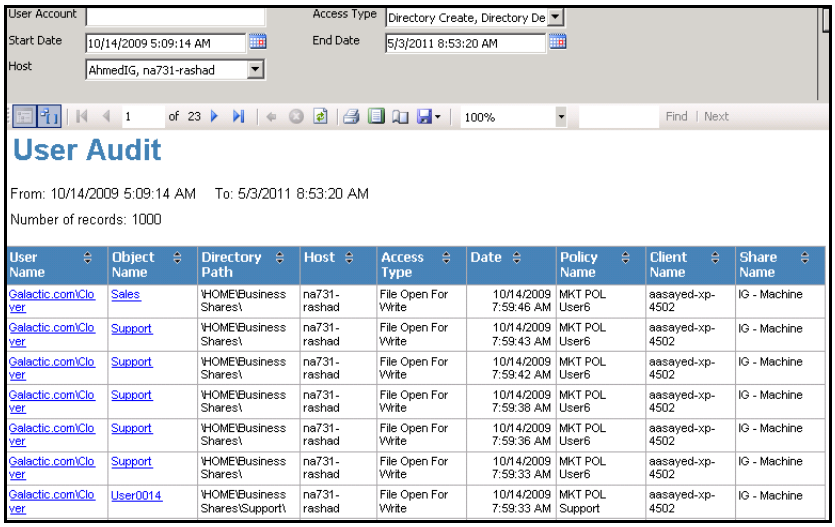
Listed as follows are the different types of reports provided by NTP Software File Auditor:

1. The **User Reports** category has four different views: the User Summary, the User Audit, the Access History, and the Most Active Users.
   a. **User Summary:** This report allows you to search by user name. Clicking on a specific user name, you can review the count of each operation performed, including the count of the deleted/renamed/moved files, the count of the created/changed/owner changed/permission changed files, the count of the created/deleted directories, and the count of the renamed directories files. In addition, it displays a list of the most-used client names, along with the count of operation(s) performed using the specified IP address.


Number of deleted files: 1
Number of changed files: 2
Number of renamed files: 2
Number of owner changed files: 2
Number of moved files: 0
Number of permission changed files: 2
Number of created files: 9
Number of deleted directories: 1
Number of renamed directories: 2
Number of created directories: 4
Last activity Date/Time: 10/14/2009 7:59:04 AM
Used Client Machine Names
Top 5 used client machines
Client Name
Number of operations done from the IP
aasayed-xp-4502
100
View All...

Copyright © 2012 by NTP Software®. All rights reserved.

b. **User Audit:** This report allows you to review all the file and directory operations performed by user(s). The report input is the user account, and/or the access type, and/or the date range, and/or the host name. The report displays the user's name, the object name, the directory path, the host name, the operation performed, the date the operation was performed, the policy name, the client, and the share name within the specified criteria.



User Account | Access Type: Directory Create, Directory De
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:53:20 AM
Host: AhmedIG, na731-rashad

1 of 23 | 100% | Find | Next

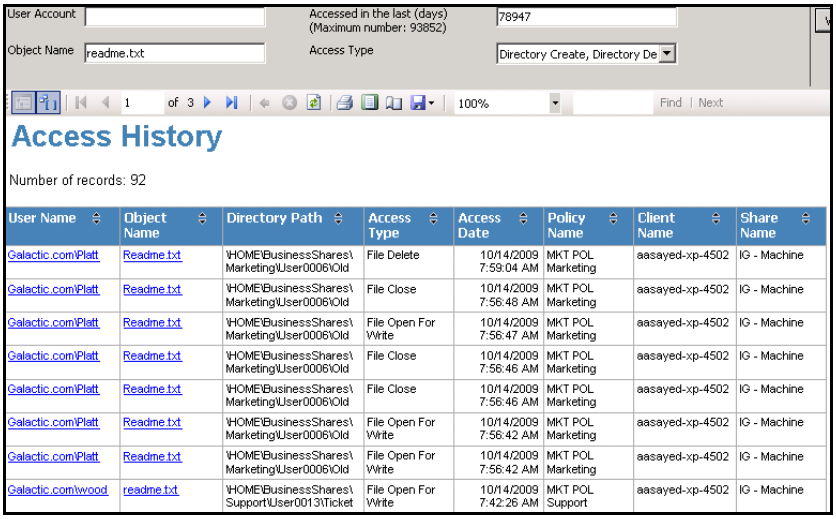
User Audit

From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:53:20 AM

Number of records: 1000

User Name	Object Name	Directory Path	Host	Access Type	Date	Policy Name	Client Name	Share Name
Galactic.com\Clover	Sales	\HOME\Business Shares\	na731-rashad	File Open For Write	10/14/2009 7:59:46 AM	MKT POL User6	aasayed-xp-4502	IG - Machine
Galactic.com\Clover	Support	\HOME\Business Shares\	na731-rashad	File Open For Write	10/14/2009 7:59:43 AM	MKT POL User6	aasayed-xp-4502	IG - Machine
Galactic.com\Clover	Support	\HOME\Business Shares\	na731-rashad	File Open For Write	10/14/2009 7:59:42 AM	MKT POL User6	aasayed-xp-4502	IG - Machine
Galactic.com\Clover	Support	\HOME\Business Shares\	na731-rashad	File Open For Write	10/14/2009 7:59:38 AM	MKT POL User6	aasayed-xp-4502	IG - Machine
Galactic.com\Clover	Support	\HOME\Business Shares\	na731-rashad	File Open For Write	10/14/2009 7:59:36 AM	MKT POL User6	aasayed-xp-4502	IG - Machine
Galactic.com\Clover	Support	\HOME\Business Shares\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	MKT POL User6	aasayed-xp-4502	IG - Machine
Galactic.com\Clover	User0014	\HOME\Business Shares\Support\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	MKT POL Support	aasayed-xp-4502	IG - Machine

c. **Access History:** This report allows you to review all the file and directory operations performed within a specified number of days. The report input is the user account, and/or the number of day(s) in which the file/directory was accessed, and/or the file name, and/or the access type performed on the file/directory. The report displays the user's name, the object name, the directory path, the operation performed, the date the operation was performed, the policy name, the client name, and the share name within the specified criteria.



User Account | Accessed in the last (days) (Maximum number: 93852): 78947
Object Name: readme.txt | Access Type: Directory Create, Directory De

1 of 3 | 100% | Find | Next

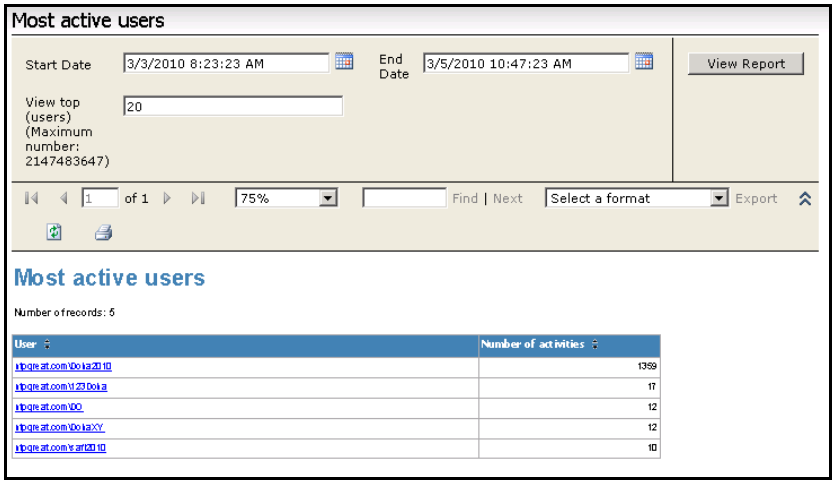
Access History

Number of records: 92

User Name	Object Name	Directory Path	Access Type	Access Date	Policy Name	Client Name	Share Name
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\Old	File Delete	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\Old	File Close	10/14/2009 7:56:48 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\Old	File Open For Write	10/14/2009 7:56:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\Old	File Close	10/14/2009 7:56:46 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\Old	File Close	10/14/2009 7:56:46 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\Old	File Open For Write	10/14/2009 7:56:42 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\Old	File Open For Write	10/14/2009 7:56:42 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\wood	readme.txt	\HOME\BusinessShares\Support\User0013\Ticket	File Open For Write	10/14/2009 7:42:26 AM	MKT POL Support	aasayed-xp-4502	IG - Machine

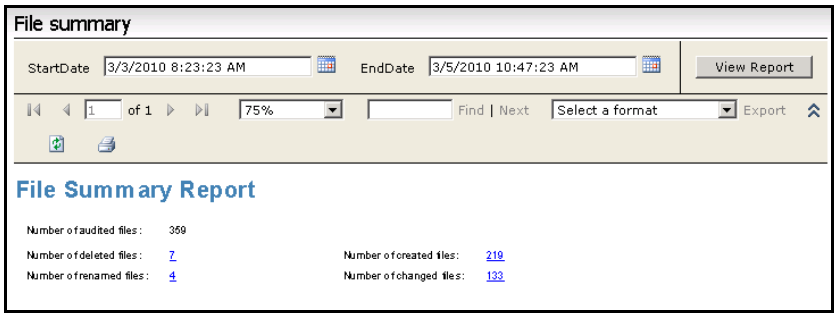
Copyright © 2012 by NTP Software®. All rights reserved.

d. **Most Active Users:** This report allows you to review the most active users with the users' activities sorted in a descending or ascending order. The report input is the date range and/or the number of most active users to view. The report displays the user name and the number of activities performed by this user within the specified criteria.



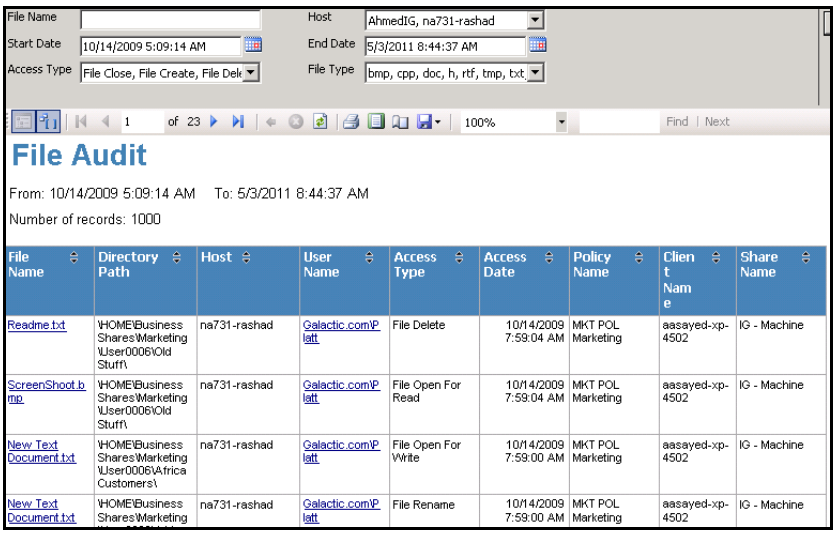
2. The **File Reports** category has nine different views: File Summary, File Audit, Files Changed, Files Deleted, Files Renamed, Files Created, Deletion Compliance, Owner Changed, and Permission Changed.

   a. **File Summary:** This report allows you to review the count of all the audited files. It also displays a breakdown for the count of deleted, renamed, created, or changed files. You can click the count next to any file operation to display a detailed list of the specified file operation.

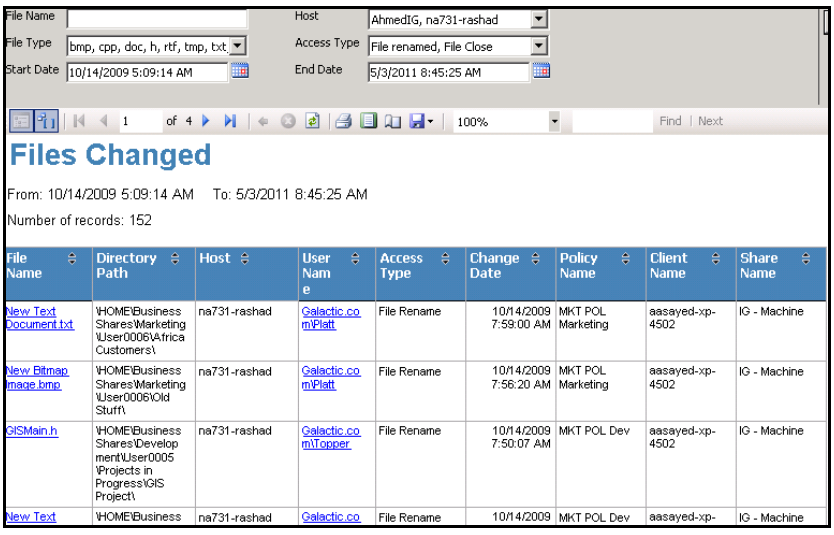


Copyright © 2012 by NTP Software®. All rights reserved.

b. **File Audit:** This report allows you to review all the file operations performed. The report input is the file name, and/or the host name, and/or the file operation performed, and/or the file type, and/or the date range. The report displays the file name, the directory name where the specified file is located, the user name accessing the file, access type, access date, the name of the policy applied on the directory, the client name, and the share name within the specified criteria.

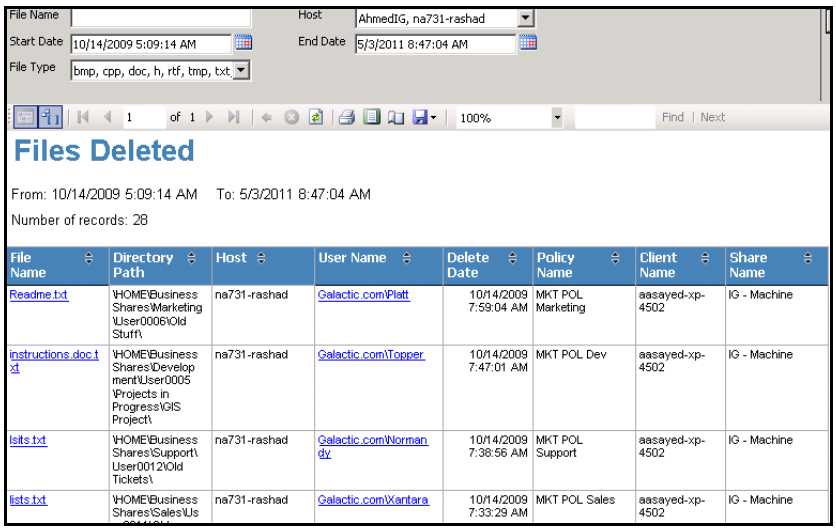

File Name
Host
AhmedIG, na731-rashad
Start Date
10/14/2009 5:09:14 AM
End Date
5/3/2011 8:44:37 AM
Access Type
File Close, File Create, File Del
File Type
bmp, cpp, doc, h, rtf, tmp, txt
of 23
100%
Find | Next
File Audit
From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:44:37 AM
Number of records: 1000
File Name | Directory Path | Host | User Name | Access Type | Access Date | Policy Name | Client Name | Share Name
Readme.txt | \HOME\Business Shares\Marketing \User0006\Old Stuff\ | na731-rashad | Galactic.com\Platt | File Delete | 10/14/2009 7:59:04 AM | MKT POL Marketing | aasayed-xp-4502 | IG - Machine
ScreenShoot.bmp | \HOME\Business Shares\Marketing \User0006\Old Stuff\ | na731-rashad | Galactic.com\Platt | File Open For Read | 10/14/2009 7:59:04 AM | MKT POL Marketing | aasayed-xp-4502 | IG - Machine
New Text Document.txt | \HOME\Business Shares\Marketing \User0006\Africa Customers\ | na731-rashad | Galactic.com\Platt | File Open For Write | 10/14/2009 7:59:00 AM | MKT POL Marketing | aasayed-xp-4502 | IG - Machine
New Text Document.txt | \HOME\Business Shares\Marketing | na731-rashad | Galactic.com\Platt | File Rename | 10/14/2009 7:59:00 AM | MKT POL Marketing | aasayed-xp-4502 | IG - Machine

c. **Files Changed:** This report allows you to view all the changed files. The report input is the file name, and/or the host name, and/or the date range, and/or the file type(s). The report displays the file name, directory path in which the file is located, the user name accessing the file, the access type, the access date, the name of the policy applied, the client name, and the share name within the specified criteria.


File Name
Host
AhmedIG, na731-rashad
File Type
bmp, cpp, doc, h, rtf, tmp, txt
Access Type
File renamed, File Close
Start Date
10/14/2009 5:09:14 AM
End Date
5/3/2011 8:45:25 AM
of 4
100%
Find | Next
Files Changed
From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:45:25 AM
Number of records: 152
File Name | Directory Path | Host | User Name | Access Type | Change Date | Policy Name | Client Name | Share Name
New Text Document.txt | \HOME\Business Shares\Marketing \User0006\Africa Customers\ | na731-rashad | Galactic.com\Platt | File Rename | 10/14/2009 7:59:00 AM | MKT POL Marketing | aasayed-xp-4502 | IG - Machine
New Bitmap Image.bmp | \HOME\Business Shares\Marketing \User0006\Old Stuff\ | na731-rashad | Galactic.com\Platt | File Rename | 10/14/2009 7:56:20 AM | MKT POL Marketing | aasayed-xp-4502 | IG - Machine
GISMain.h | \HOME\Business Shares\Development\User0005 \Projects in Progress\GIS Project\ | na731-rashad | Galactic.com\Topper | File Rename | 10/14/2009 7:50:07 AM | MKT POL Dev | aasayed-xp-4502 | IG - Machine
New Text | \HOME\Business | na731-rashad | Galactic.co | File Rename | 10/14/2009 | MKT POL Dev | aasayed-xp- | IG - Machine

Copyright © 2012 by NTP Software®. All rights reserved.

d. **Files Deleted:** This report allows you to review all the files that have been deleted. The report's input is the file name, and/or the host name, and/or the date range, and/or the file type. The report displays the file name, the directory path in which the file was located, the user name, the date the file was last accessed, the policy name, the client name, and the share name within the specified criteria.



File Name | Host: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:47:04 AM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

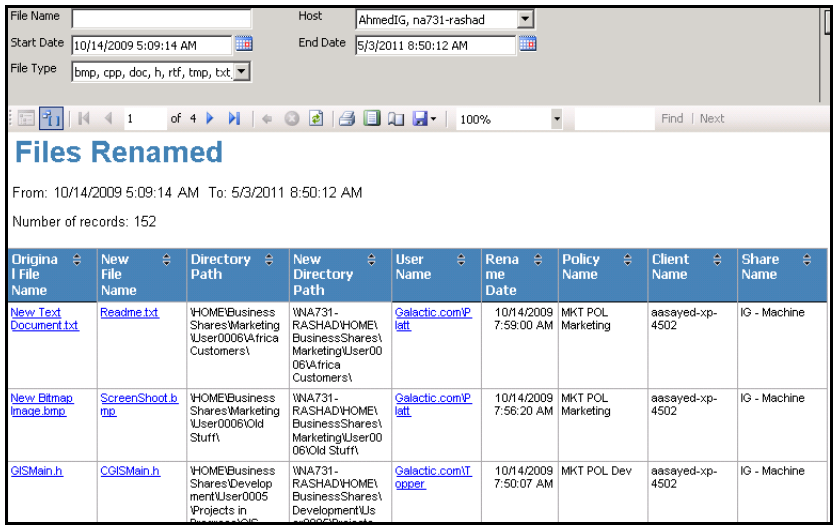
Files Deleted

From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:47:04 AM

Number of records: 28

File Name	Directory Path	Host	User Name	Delete Date	Policy Name	Client Name	Share Name
Readme.txt	\HOME\Business Shares\Marketing \User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
instructions.doc.txt	\HOME\Business Shares\Development\User0005 \Projects in Progress\GIS Project\	na731-rashad	Galactic.com\Topper	10/14/2009 7:47:01 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine
lsits.txt	\HOME\Business Shares\Support\ User0012\Old Tickets\	na731-rashad	Galactic.com\Normandy	10/14/2009 7:38:56 AM	MKT POL Support	aasayed-xp-4502	IG - Machine
lists.txt	\HOME\Business Shares\Sales\Us	na731-rashad	Galactic.com\Xantara	10/14/2009 7:33:29 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine

e. **Files Renamed:** This type of report allows you to review all the files that have been renamed. The report's input is the file name and/or, the host machine name, and/or the date range, and/or the file type. The report displays the original file name before the change, the new file name after the rename, the directory path in which the file is located, the user name, the date the file was accessed, the policy name, the client name, and the share name within the specified criteria.



File Name | Host: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:50:12 AM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

Files Renamed

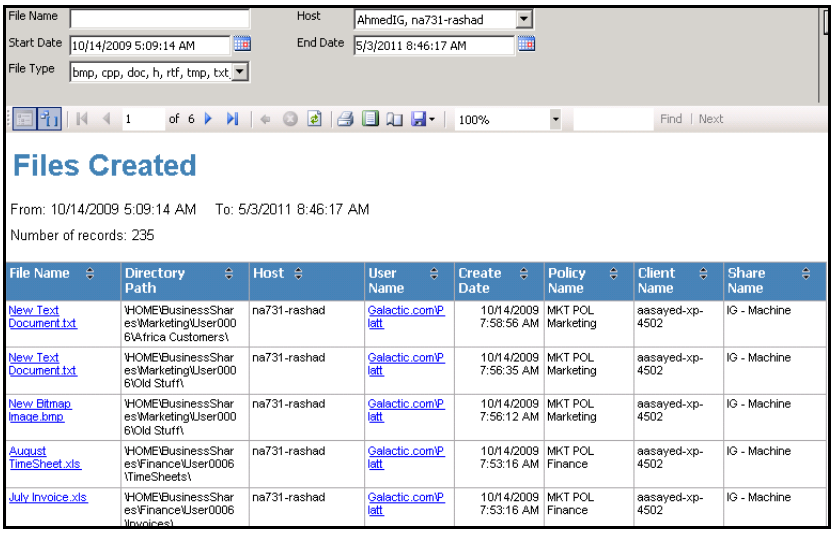
From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:50:12 AM

Number of records: 152

Original File Name	New File Name	Directory Path	New Directory Path	User Name	Rename Date	Policy Name	Client Name	Share Name
New Text Document.txt	Readme.txt	\HOME\Business Shares\Marketing \User0006\Africa Customers\	\\NA731-RASHAD\HOME\ BusinessShares\ Marketing\User0006\Africa Customers\	Galactic.com\Platt	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Bitmap Image.bmp	ScreenShoot.bmp	\HOME\Business Shares\Marketing \User0006\Old Stuff\	\\NA731-RASHAD\HOME\ BusinessShares\ Marketing\User0006\Old Stuff\	Galactic.com\Platt	10/14/2009 7:56:20 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
GISMain.h	CGISMain.h	\HOME\Business Shares\Development\User0005 \Projects in	\\NA731-RASHAD\HOME\ BusinessShares\ Development\Us	Galactic.com\Topper	10/14/2009 7:50:07 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine

Copyright © 2012 by NTP Software®. All rights reserved.

f. **Files Created:** This type of report allows you to review all the files that have been created. The report's input is the date range, and/or the file name, and/or the file type, and/or the user account. The report displays the file name, the directory path in which the file exists, the user name, the access type (which is "file create"), the access date, the policy name, the client name, and the share name within the specified criteria.



File Name | Host: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:46:17 AM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

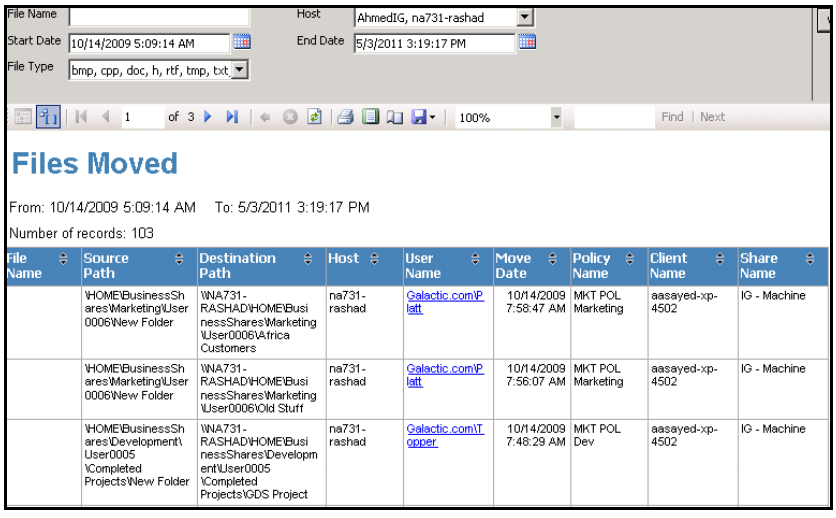
Files Created

From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:46:17 AM

Number of records: 235

File Name	Directory Path	Host	User Name	Create Date	Policy Name	Client Name	Share Name
New Text Document.txt	\HOME\BusinessShares\Marketing\User0006\Africa Customers\	na731-rashad	Galactic.com\Platt	10/14/2009 7:58:56 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Text Document.txt	\HOME\BusinessShares\Marketing\User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:35 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Bitmap Image.bmp	\HOME\BusinessShares\Marketing\User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:12 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
August TimeSheet.xls	\HOME\BusinessShares\Finance\User0006\TimeSheets\	na731-rashad	Galactic.com\Platt	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
July Invoice.xls	\HOME\BusinessShares\Finance\User0006\Invoices\	na731-rashad	Galactic.com\Platt	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine

g. **Files Moved:** This type of report allows you to review all the files that have been moved. The report's input is the date range, and/or the file name, and/or the file type, and/or the host name. The report displays the file name, the source path and the destination path of the moved file, the host name, the date on which the file was moved, the policy name, the machine IP address, and the share name within the specified criteria.



File Name | Host: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 3:19:17 PM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

Files Moved

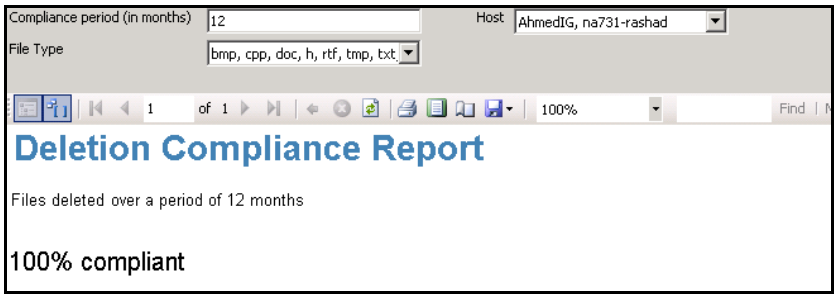
From: 10/14/2009 5:09:14 AM To: 5/3/2011 3:19:17 PM

Number of records: 103

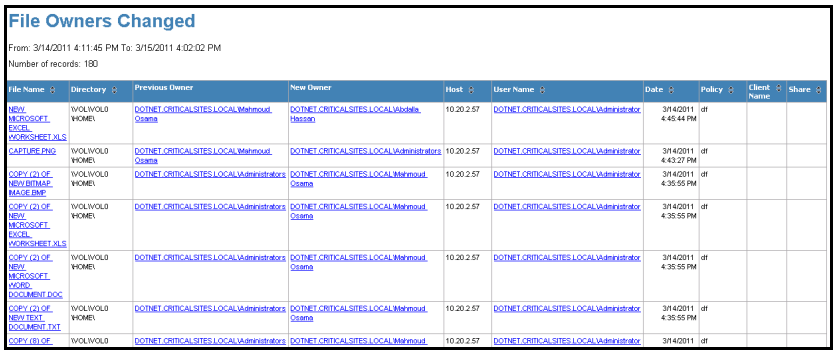
File Name	Source Path	Destination Path	Host	User Name	Move Date	Policy Name	Client Name	Share Name
	\HOME\BusinessShares\Marketing\User0006\New Folder	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Africa Customers	na731-rashad	Galactic.com\Platt	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
	\HOME\BusinessShares\Marketing\User0006\New Folder	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Old Stuff	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
	\HOME\BusinessShares\Development\User0005\Completed Projects\New Folder	\\NA731-RASHAD\HOME\BusinessShares\Development\User0005\Completed Projects\GDS Project	na731-rashad	Galactic.com\Topper	10/14/2009 7:48:29 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine

Copyright © 2012 by NTP Software®. All rights reserved.

h. **Deletion Compliance:** This type of report allows you to review the files deleted over the specified compliance period. The report's input is the compliance period in months, the host name, and the file type. The report displays the files deleted over the specified period.



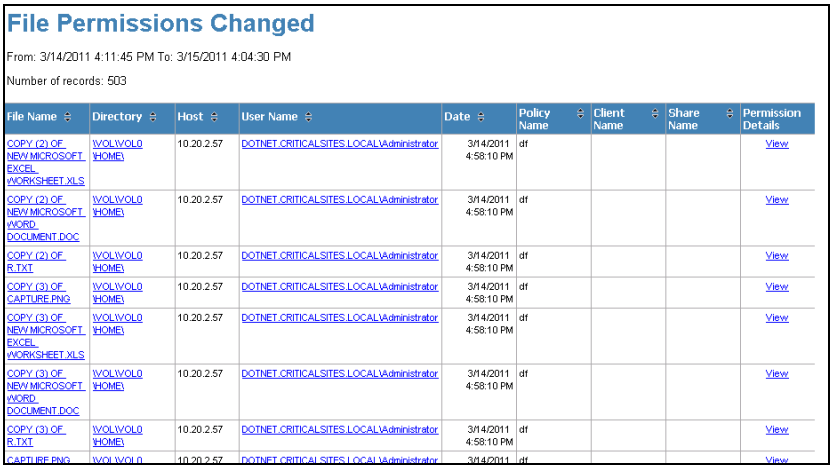
i. **Owner Changed:** This type of report allows you to review the file(s) whose owner(s) has changed. The report displays the name of the file whose owner has changed, the previous owner, the new owner, the host IP address, the user name, the policy name, the client, and the share name within the specified criteria.



File Name	Directory	Previous Owner	New Owner	Host	User Name	Date	Policy	Client Name	Share
NEW MICROSOFT EXCEL WORKSHEET.XLS	\\VOL1\VOL0 HOME\	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	DOTNET.CRITICALSITES.LOCAL\Abdalla Hassan	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:45:44 PM	df		
CAPTURE.PNG	\\VOL1\VOL0 HOME\	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	DOTNET.CRITICALSITES.LOCAL\Administrators	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:43:27 PM	df		
COPY (2) OF NEW BITMAP IMAGE.BMP	\\VOL1\VOL0 HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	\\VOL1\VOL0 HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW MICROSOFT WORD DOCUMENT.DOC	\\VOL1\VOL0 HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW TEXT DOCUMENT.TXT	\\VOL1\VOL0 HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (8) OF	\\VOL1\VOL0	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011	df		

Copyright © 2012 by NTP Software®. All rights reserved.

j. **Permission Changed:** This type of report allows you to review the file(s) whose permission(s) has changed among user. The report displays the name of the file whose permission has changed, the directory where the file exists, the host IP address, the user name, the policy name, the client, and the share name, as well as the permission details within the specified criteria.



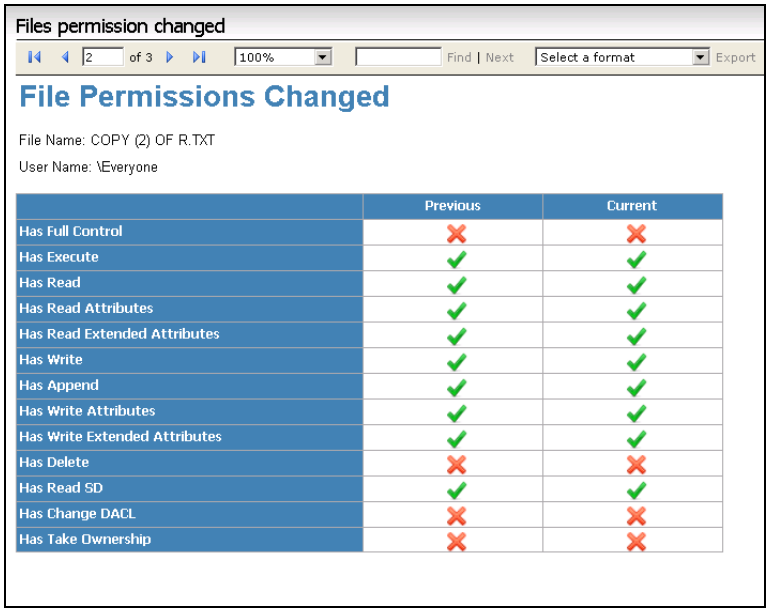
File Permissions Changed

From: 3/14/2011 4:11:45 PM To: 3/15/2011 4:04:30 PM

Number of records: 503

File Name	Directory	Host	User Name	Date	Policy Name	Client Name	Share Name	Permission Details
COPY (2) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (2) OF NEW MICROSOFT WORD DOCUMENT.DOC	\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (2) OF R.TXT	\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (3) OF CAPTURE.PNG	\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (3) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (3) OF NEW MICROSOFT WORD DOCUMENT.DOC	\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (3) OF R.TXT	\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
CAPTURE.PNG	\VOL\VOL0	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011	df			View

Clicking on the **View** link of the **Permission Details** field displays more details, as outlined below.



Files permission changed

2 of 3 100% Find | Next Select a format Export

File Permissions Changed

File Name: COPY (2) OF R.TXT

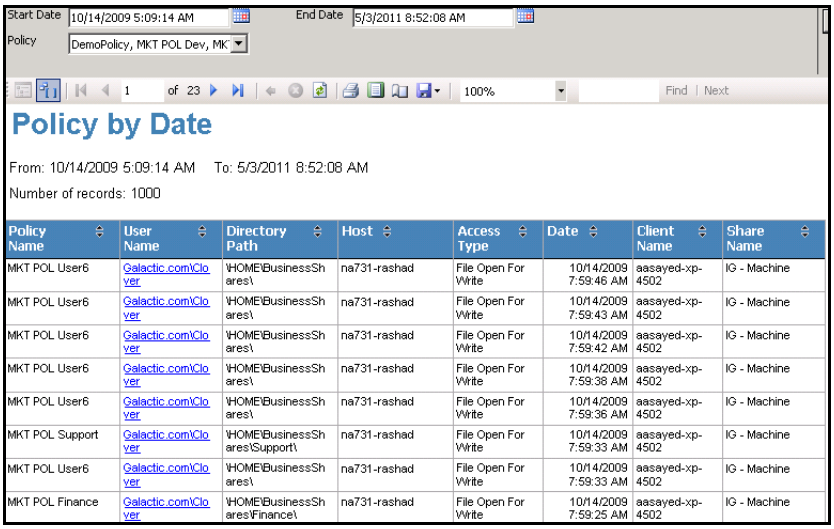
User Name: \Everyone

	Previous	Current
Has Full Control	✗	✗
Has Execute	✓	✓
Has Read	✓	✓
Has Read Attributes	✓	✓
Has Read Extended Attributes	✓	✓
Has Write	✓	✓
Has Append	✓	✓
Has Write Attributes	✓	✓
Has Write Extended Attributes	✓	✓
Has Delete	✗	✗
Has Read SD	✓	✓
Has Change DACL	✗	✗
Has Take Ownership	✗	✗

Copyright © 2012 by NTP Software®. All rights reserved.

3. **Policy Reports** category has one view: the Policy by Date report.

   a. **Policy by Date:** This report allows you to review all the policy details within a certain date range. The report's input is the date range and/or the policy name. The report displays the policy name, the user name, the directory path on which the policy applies, the access type, the access date, the machine IP address, and the share name within the specified criteria.


Start Date 10/14/2009 5:09:14 AM End Date 5/3/2011 8:52:08 AM
Policy DemoPolicy, MKT POL Dev, MK
1 of 23 100% Find | Next

Policy by Date

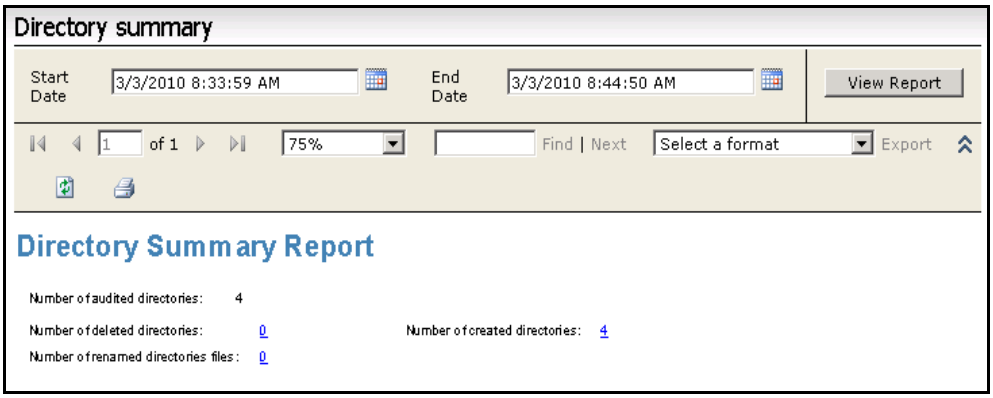
From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:52:08 AM

Number of records: 1000

Policy Name	User Name	Directory Path	Host	Access Type	Date	Client Name	Share Name
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:46 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:43 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:42 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:38 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:36 AM	aasayed-xp-4502	IG - Machine
MKT POL Support	Galactic.com\Clover	\HOME\BusinessShares\Support\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	aasayed-xp-4502	IG - Machine
MKT POL Finance	Galactic.com\Clover	\HOME\BusinessShares\Finance\	na731-rashad	File Open For Write	10/14/2009 7:59:25 AM	aasayed-xp-4502	IG - Machine

4. The **Directory Reports** category has eight views: Directory Summary, Directory Audit, Directory Created, Directory Renamed, Directory Deleted, Deleted Files by Folder, Deleted Files Count by Folder, and Most Accessed Folders.

   a. **Directory Summary:** This report allows you to review the count of all the audited directories. It also displays a breakdown for the count of deleted, renamed, or created directories. You can click the count next to any directory operation to display a detailed list of the specified directory operation.


Directory summary

Start Date 3/3/2010 8:33:59 AM End Date 3/3/2010 8:44:50 AM View Report

1 of 1 75% Find | Next Select a format Export

Directory Summary Report

Number of audited directories: 4

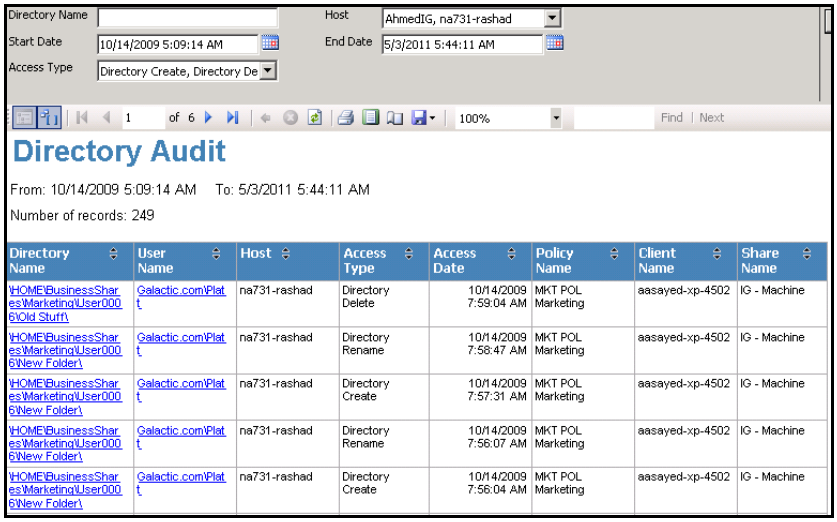
Number of deleted directories: 0

Number of created directories: 4

Number of renamed directories files: 0

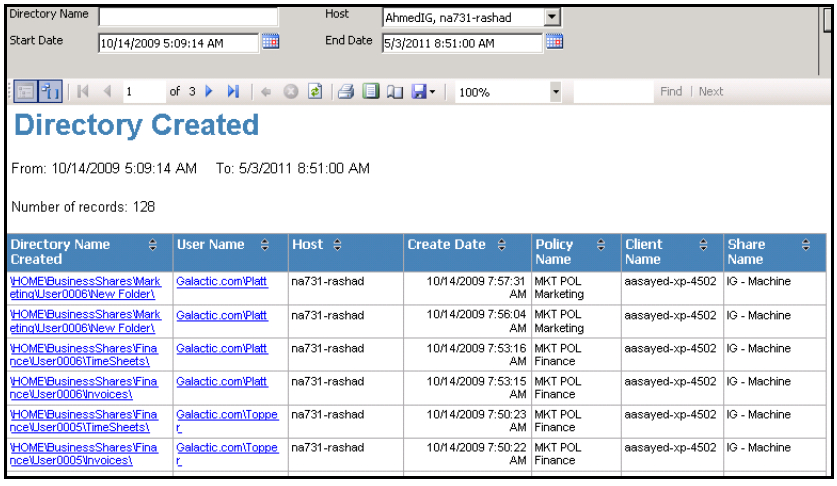
Copyright © 2012 by NTP Software®. All rights reserved.

b. **Directory Audit:** This report allows you to review all the directory operations performed. The report's input is the directory name, and/or the host name, and/or the date range, and/or the access type. The report displays the directory name, the user name accessing the directory, access type, access date, the name of the policy applied on the directory, the client name, and the share name. You can choose to display the previous information within a certain date range and/or for a certain access type(s) and/or for a certain directory name.



Directory Name	User Name	Host	Access Type	Access Date	Policy Name	Client Name	Share Name
\HOME\BusinessShares\Marketing\User0006\Old Stuff\	Galactic.com\Platt	na731-rashad	Directory Delete	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Rename	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Create	10/14/2009 7:57:31 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Rename	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Create	10/14/2009 7:56:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine

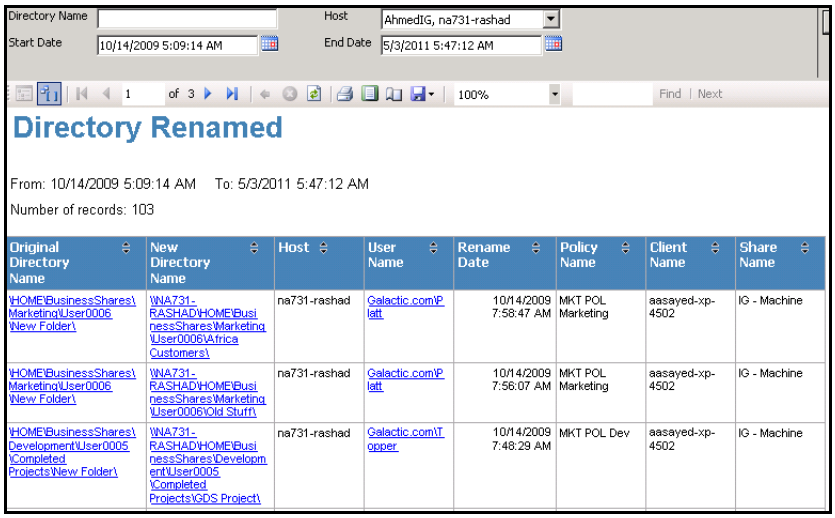
c. **Directory Created:** This report allows you to review all the directories created. The report's input is the date range, and/or the directory name, and/or the host name. The report displays the name of the created directory, the user's name performing the directory create operation, the date in which the directory was created, the name of the policy governing this directory creation operation, the IP address of the machine used to perform the directory create operation, and the share name based on the specified criteria.



Directory Name Created	User Name	Host	Create Date	Policy Name	Client Name	Share Name
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	10/14/2009 7:57:31 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	10/14/2009 7:56:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0006\TimeSheets\	Galactic.com\Platt	na731-rashad	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0006\Invoices\	Galactic.com\Platt	na731-rashad	10/14/2009 7:53:15 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0005\TimeSheets\	Galactic.com\Topper	na731-rashad	10/14/2009 7:50:23 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0005\Invoices\	Galactic.com\Topper	na731-rashad	10/14/2009 7:50:22 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine

Copyright © 2012 by NTP Software®. All rights reserved.

d. **Directory Renamed:** This report allows you to review all the renamed directories. The report's inputs are the directory name, and/or the host name, and/or the date range. The report displays the original directory name before the renaming operation, the new directory name after renaming, the user's name performing the directory rename operation, the date on which the directory was renamed, the name of the policy governing this directory rename operation, the IP address of the machine used to perform the directory rename operation, and the share name based on the specified criteria.


Directory Name
Host
AhmedIG, na731-rashad
Start Date
10/14/2009 5:09:14 AM
End Date
5/3/2011 5:47:12 AM
1 of 3
100%
Find | Next

Directory Renamed

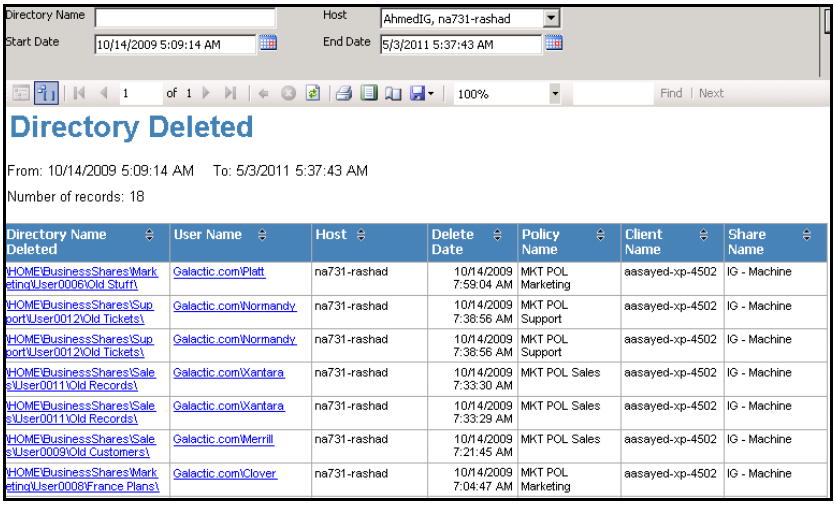
From: 10/14/2009 5:09:14 AM To: 5/3/2011 5:47:12 AM

Number of records: 103

Original Directory Name	New Directory Name	Host	User Name	Rename Date	Policy Name	Client Name	Share Name
\HOME\BusinessShares\Marketing\User0006\New Folder\	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Africa Customers\	na731-rashad	Galactic.com\Platt	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Development\User0005\Completed Projects\New Folder\	\\NA731-RASHAD\HOME\BusinessShares\Development\User0005\Completed Projects\GDS Project\	na731-rashad	Galactic.com\Topper	10/14/2009 7:48:29 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine

Copyright © 2012 by NTP Software®. All rights reserved.

e. **Directory Deleted:** This report allows you to review all the deleted directories. The report's input is the date range, and/or the directory name, and/or the host name. The report displays the name of the deleted directory, the user's name performing the directory delete operation, the date in which the directory was deleted, the name of the policy governing this directory deletion operation, the client name used to perform the directory delete operation, and the share name based on the specified criteria.



Directory Name | Host: AhmedIG, na731-rashad | Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 5:37:43 AM

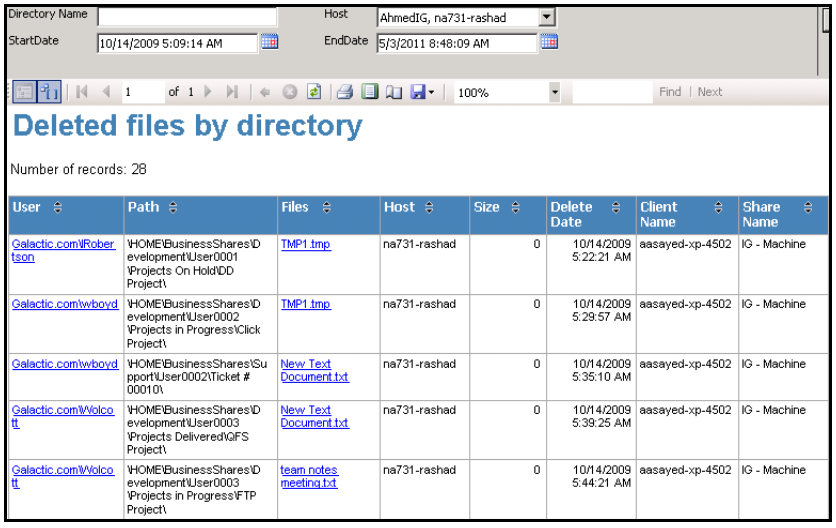
Directory Deleted

From: 10/14/2009 5:09:14 AM To: 5/3/2011 5:37:43 AM

Number of records: 18

Directory Name Deleted	User Name	Host	Delete Date	Policy Name	Client Name	Share Name
\HOME\BusinessShares\Marketing\User0006\Old Stuff\	Galactic.com\Platt	na731-rashad	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Support\User0012\Old Tickets\	Galactic.com\Normandy	na731-rashad	10/14/2009 7:38:56 AM	MKT POL Support	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Support\User0012\Old Tickets\	Galactic.com\Normandy	na731-rashad	10/14/2009 7:38:56 AM	MKT POL Support	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Sales\User0011\Old Records\	Galactic.com\Xantara	na731-rashad	10/14/2009 7:33:30 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Sales\User0011\Old Records\	Galactic.com\Xantara	na731-rashad	10/14/2009 7:33:29 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Sales\User0009\Old Customers\	Galactic.com\Merrill	na731-rashad	10/14/2009 7:21:45 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0008\France Plans\	Galactic.com\Clover	na731-rashad	10/14/2009 7:04:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine

f. **Deleted Files by Directory:** This report allows you to review all the deleted files grouped by directory. The report's input is the directory name, and/or the host, and/or the date range. The report displays the user's name who has deleted the file(s), the path from which the file was deleted, the file name, the host name, the file size, the date on which the file was deleted, the client name used to perform the file delete operation, and the share name based on the specified criteria.



Directory Name | Host: AhmedIG, na731-rashad | StartDate: 10/14/2009 5:09:14 AM | EndDate: 5/3/2011 8:48:09 AM

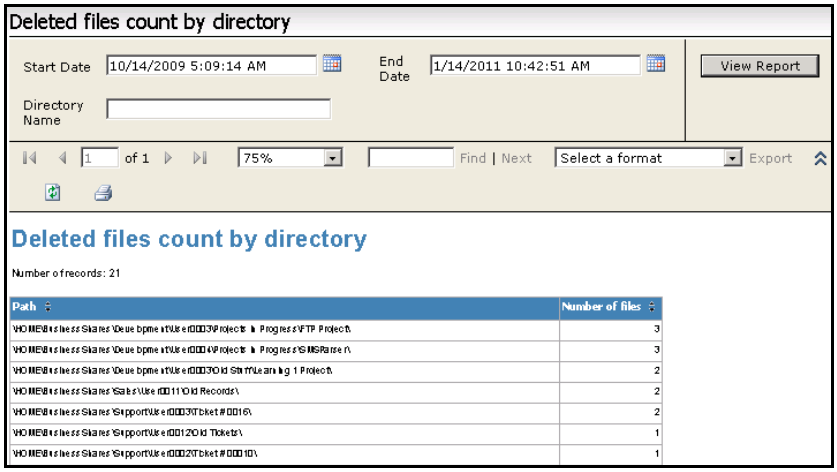
Deleted files by directory

Number of records: 28

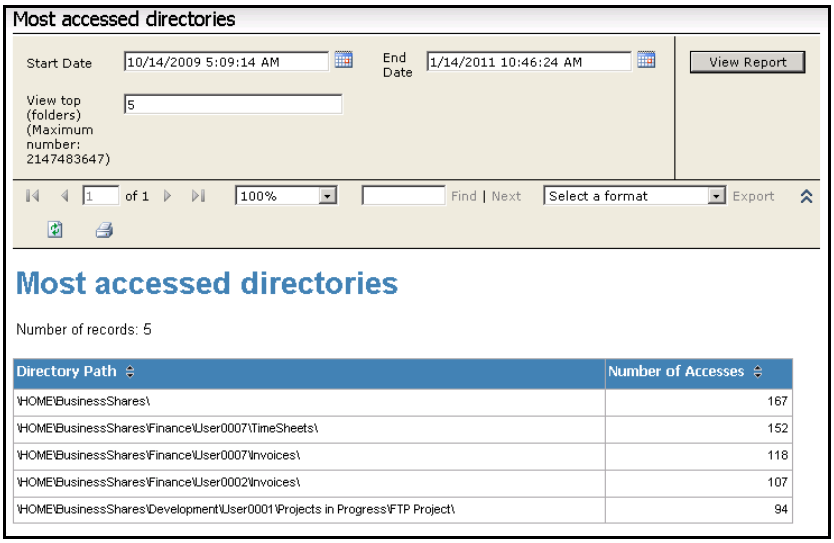
User	Path	Files	Host	Size	Delete Date	Client Name	Share Name
Galactic.com\Robertson	\HOME\BusinessShares\Development\User0001\Projects On Hold\DD Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:22:21 AM	aasayed-xp-4502	IG - Machine
Galactic.com\wboyd	\HOME\BusinessShares\Development\User0002\Projects in Progress\Click Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:29:57 AM	aasayed-xp-4502	IG - Machine
Galactic.com\wboyd	\HOME\BusinessShares\Support\User0002\Ticket # 00010\	New Text Document.txt	na731-rashad	0	10/14/2009 5:35:10 AM	aasayed-xp-4502	IG - Machine
Galactic.com\Volcott	\HOME\BusinessShares\Development\User0003\Projects Delivered\QFS Project\	New Text Document.txt	na731-rashad	0	10/14/2009 5:39:25 AM	aasayed-xp-4502	IG - Machine
Galactic.com\Volcott	\HOME\BusinessShares\Development\User0003\Projects in Progress\FTP Project\	team notes meeting.txt	na731-rashad	0	10/14/2009 5:44:21 AM	aasayed-xp-4502	IG - Machine

Copyright © 2012 by NTP Software®. All rights reserved.

g. **Deleted Files Count by Directory:** This report allows you to review the number of deleted files with a directory. The report's input is the date range and/or the directory name. The report displays the folder path and the number of files deleted within the specified directory/directories within the specified date range.

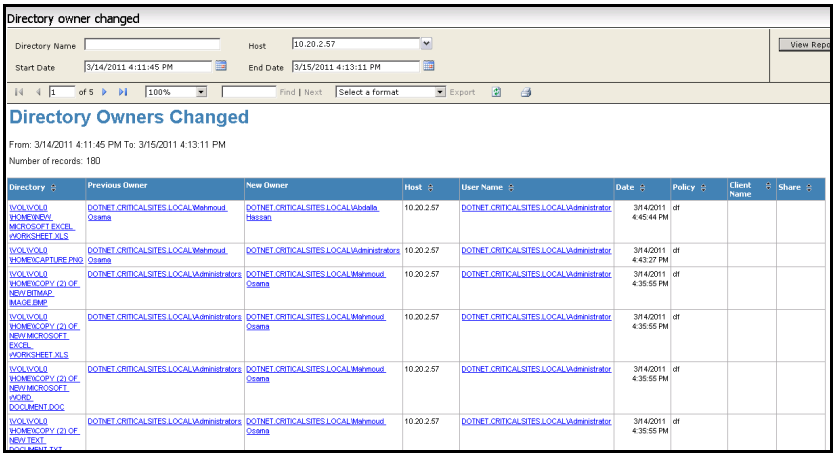


h. **Most Accessed Directories:** This report allows you to review the most-accessed directories. The report's input is the date range, and/or number of most-accessed directories to display. The report displays the directory path and the number of times each directory was accessed.

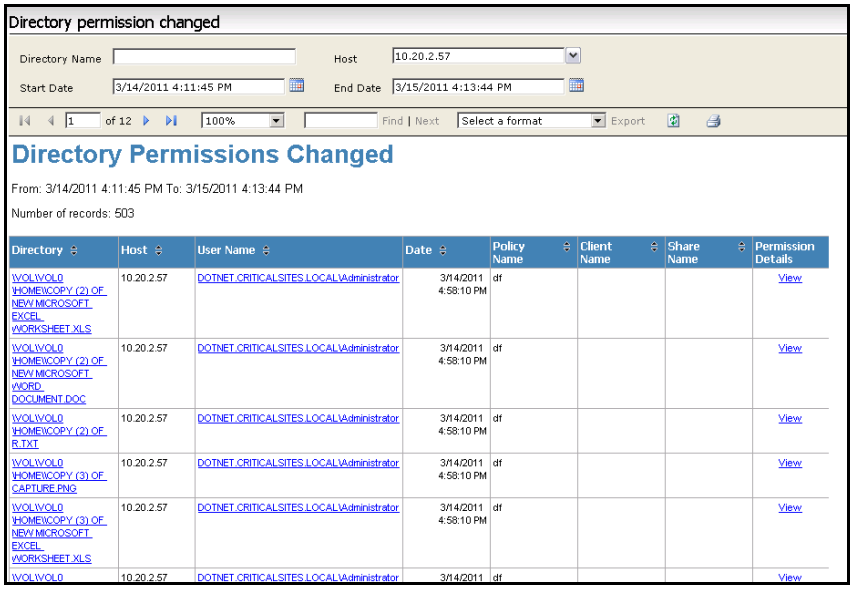


Copyright © 2012 by NTP Software®. All rights reserved.

i. **Directory Owner Changed:** This report allows you to review all directories whose owners have changed. The report displays the directory name, the previous and new owners, the host IP address, the user name, the date, the policy name, the client name, and the share name based on the specified criteria.

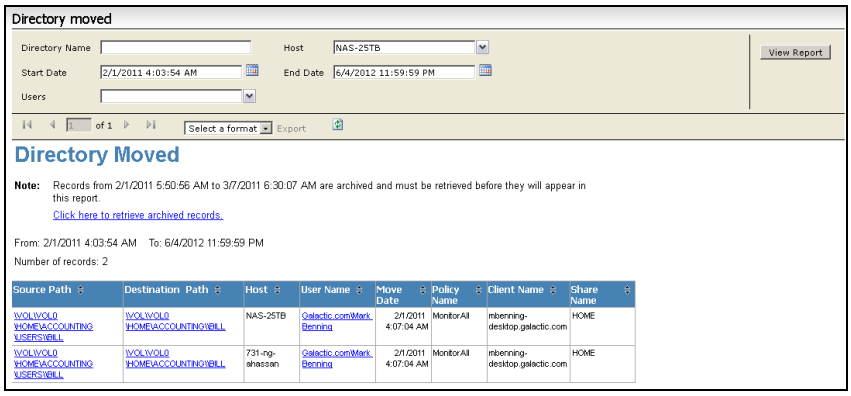


j. **Directory Permission Changed:** This report allows you to review all directories whose permissions have changed. The report displays the directory name, the host IP address, the user name, the date, the policy name, the client name, the share name, and the permission details based on the specified criteria.



Copyright © 2012 by NTP Software®. All rights reserved.

k. **Directory Moved:** This report allows you to review all directories that have moved. The report displays the source path, the destination path, the host name, the user name, the date the directory was moved, the policy name, the client name, and the share name.

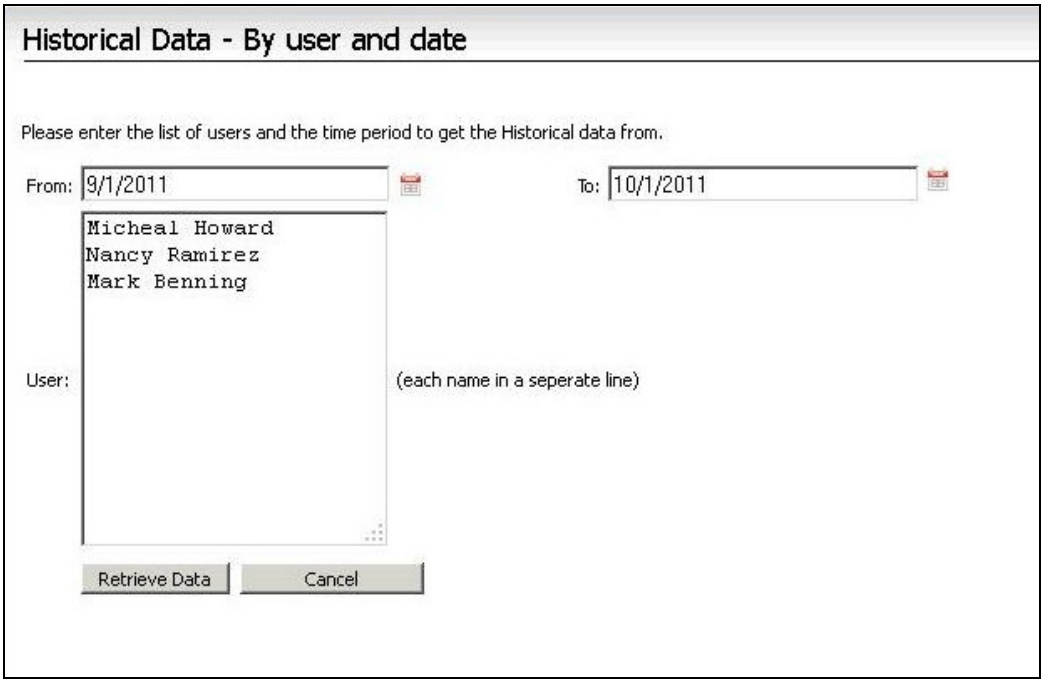


Copyright © 2012 by NTP Software®. All rights reserved.

Retrieving Records Archived via ODDM

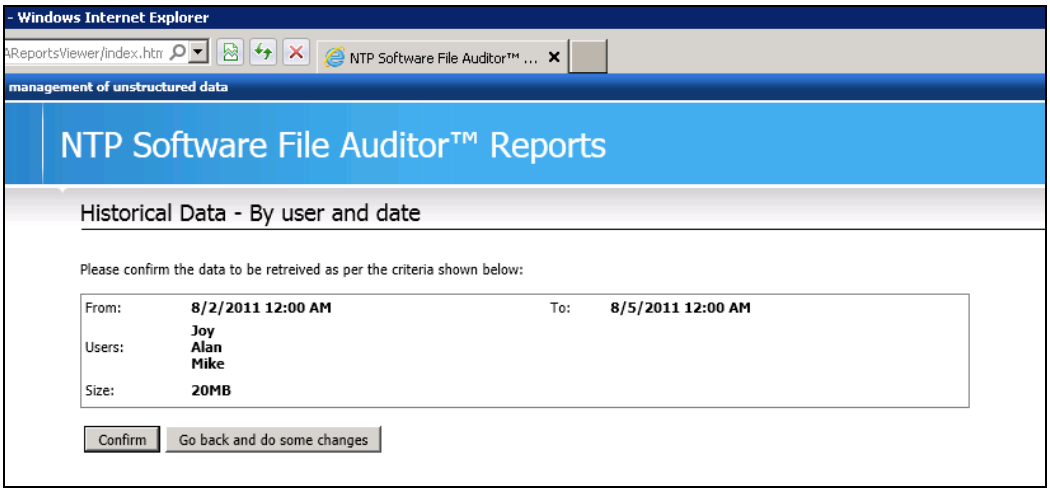
There are two methods to retrieve the archived records; the first method is as follows:

1. Run NTP Software File Auditor Administrator by clicking **Start** > **All Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor Reports**.
2. Click **Prepare Historical Data**.
3. Specify the time period and the user(s) you wish to retrieve their activities. Click the **Retrieve Data** button.



Copyright © 2012 by NTP Software®. All rights reserved.

4. File Auditor displays the specified date range, the specified users and calculates the overall size of the data retrieved for the DX server. Review the details and click **Confirm** to proceed.



NOTE: Please make sure your primary SQL Server has enough space for the retrieved data before you press the **Confirm** button.

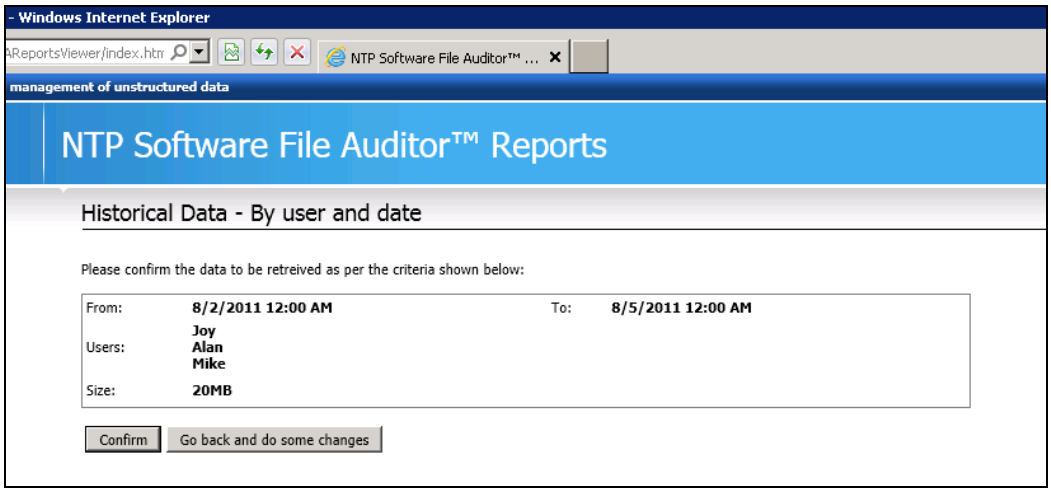
5. File Auditor will retrieve the old data and insert it in the same database that File Auditor uses.
6. You can now select any report, and the report results will contain the historical data.

Copyright © 2012 by NTP Software®. All rights reserved.

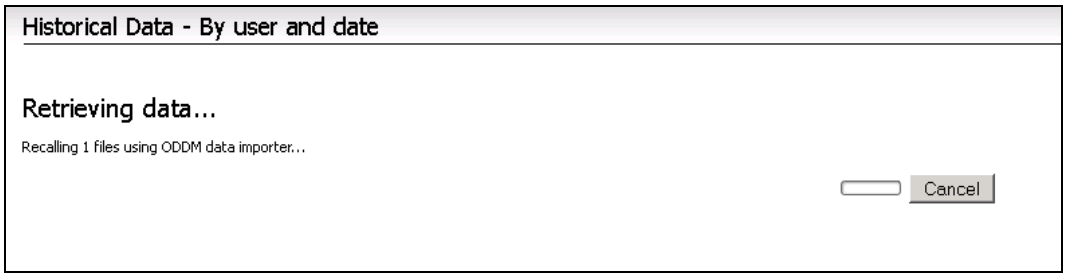
The second method is as follows:

1. Run NTP Software File Auditor Administrator by clicking **Start** > **All Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor Reports**.
2. Select any report you wish to view, specify the report input, and click **View Report**.
3. File Auditor Reports will look up the database to see if there are any archived files based on the criteria specified.
4. If archived data exists that has not previously been retrieved, File Auditor will display the following note:

   Note: Records from "oldest Archived record" to "newest archived record" are archived and must be retrieved before they will appear in this report. Click Here to retrieve archived records.
5. Click the **Click Here to retrieve archived records** option and File Auditor will display the specified date range and the specified users and will calculate the overall size of the data retrieved for the DX server. Review the details and click **Confirm** to proceed.

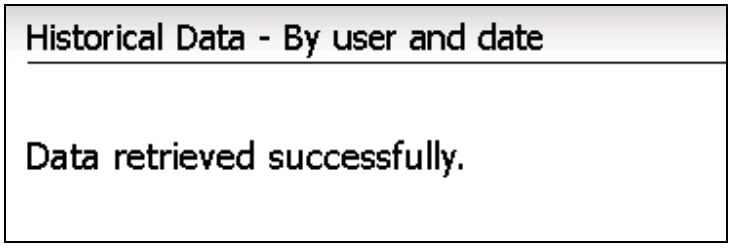

- Windows Internet Explorer
NTP Software File Auditor™ ...
management of unstructured data
NTP Software File Auditor™ Reports
Historical Data - By user and date
Please confirm the data to be retreived as per the criteria shown below:
From: 8/2/2011 12:00 AM
To: 8/5/2011 12:00 AM
Users: Joy Alan Mike
Size: 20MB
Confirm
Go back and do some changes

6. A progress dialog will show the progress of the data retrieval.



Copyright © 2012 by NTP Software®. All rights reserved.

7. Once the data has been retrieved, please close the dialog box and rerun the report.



8. The report will show the date with the archived records included.

Copyright © 2012 by NTP Software®. All rights reserved.

File Auditor Business Overwatch Tasks (BOTs)

File Auditor Business Overwatch Tasks (BOTs) are configured to run regularly against the File Auditor database to detect users' unexpected behavior.

For example, BOTs can warn administrators when a user downloads hundreds of files or gain access to secure or sensitive information; they can also warn of hacking attacks when a user deletes important files, etc.

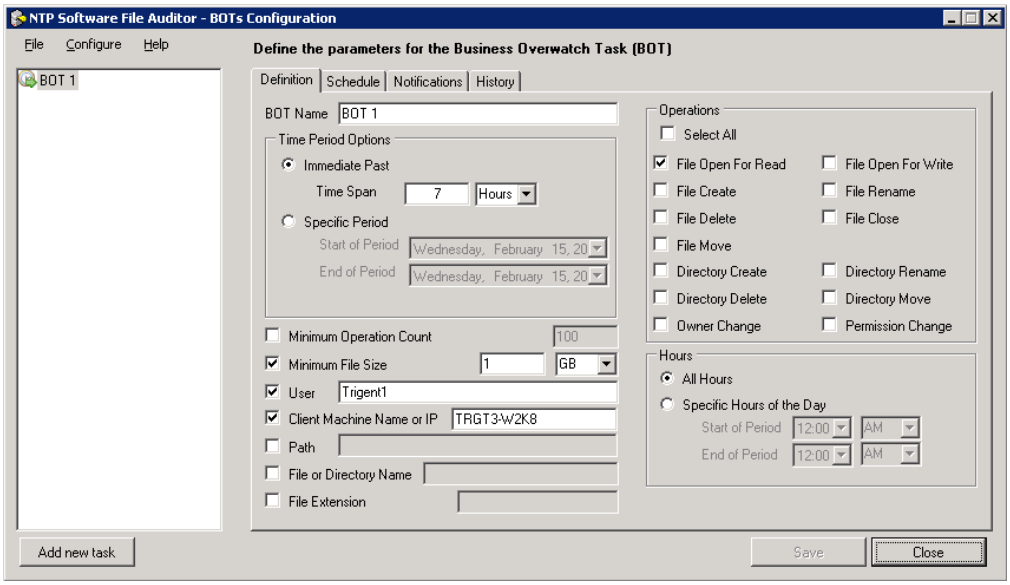
When a BOT runs, it searches the database for a specified user activity and notifies administrators accordingly via email.

NOTE: For File Auditor BOTs to function properly, a File Auditor policy must exist that monitors your NAS Device and is configured to store users' activity into a database.

Defining or Editing a BOT

A BOT has the following main parameters.

1. Definition
2. Schedule
3. Notifications

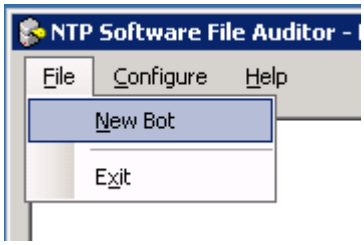


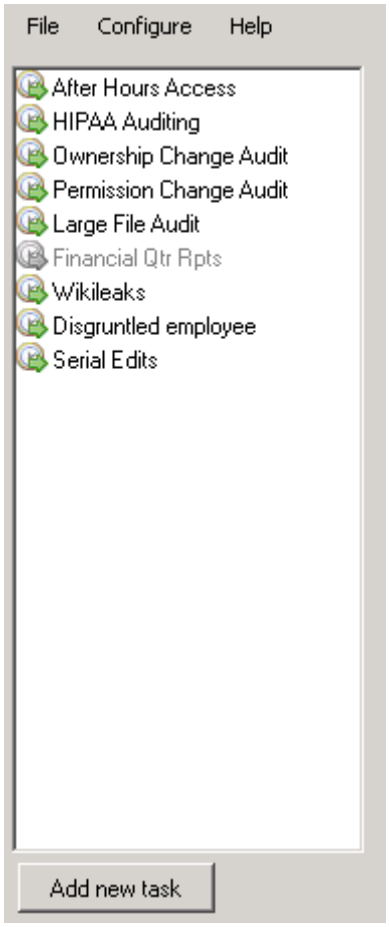
Copyright © 2012 by NTP Software®. All rights reserved.

To define a new BOT or edit an existing one, please perform the following steps:

1. On the **Start** menu, navigate to **Programs > NTP Software File Auditor > NTP Software File Auditor BOT configuration**.

2. Click the **Add New Task** button or **File > New BOT** or select an existing BOT to edit from the list on the left panel.





Copyright © 2012 by NTP Software®. All rights reserved.

3. On the **Definition** tab, specify the BOT name.

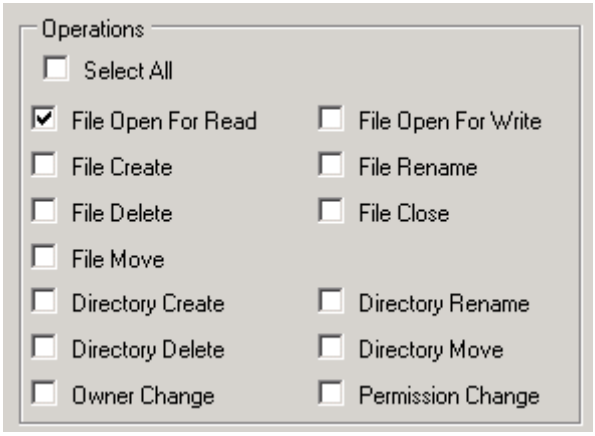
4. Use the **Time Period Options** to set the scanning period.

NOTES:

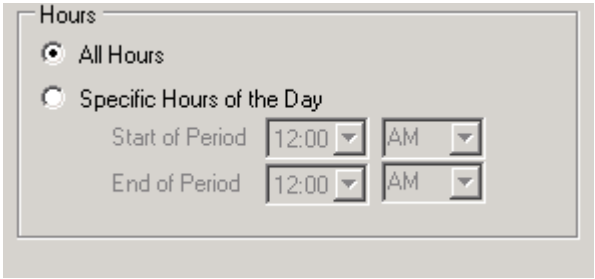
a. Set the Time Period to 'Immediate Past' if you wish to notify the user of all the matching operations that occurred in a past period.

b. Set the Time Period to 'Specific Period' if you wish to notify the user of all the matching operations that occurred within a specific time period, ignoring any operations that occurred at any other time.

5. Use the **Operations** section to check the operations you want the BOT to monitor. You can either check all operations or select individual operations to monitor.

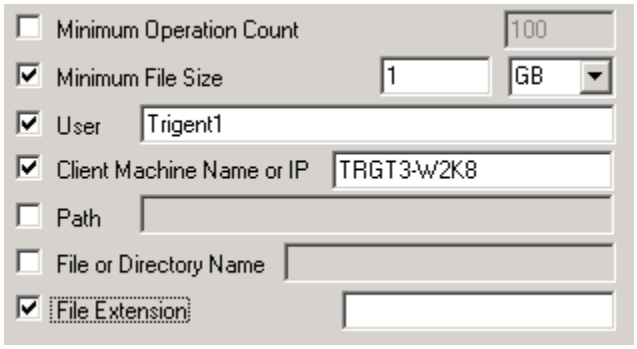


6. Use the **Hours** section to specify the scanning exact time.



Copyright © 2012 by NTP Software®. All rights reserved.

7. You can specify additional criteria for other operations details such as file extensions, the user who performed the operation, etc.



Copyright © 2012 by NTP Software®. All rights reserved.

NOTES:

a. The 'Minimum Operation Count' defines the minimum number of operations that should match for the BOT to notify the user.

b. The 'Minimum File Size' defines the minimum file size that counts as an operation for the BOT.

c. The 'User' defines the full name of the user a BOT monitors.

   Leave this field blank if you wish to search for all operations done by all users. This field does not accept account names and does not accept group names, only full names are accepted. Wildcards (* and ?) can be used (e.g., you can enter "Mark *", which will match all users whose first name is Mark).

d. The 'Client System name or IP' defines the computer name/IP a BOT monitors.

   Leave this field blank to monitor access from all computers.This field accepts only one computer name or one IP. Wildcards are used. Examples :

- To match a range of IPs, the IP can be entered as "10.20.2.*", this will match any IP in the range 10.20.2.0 to 10.20.2.255.
- To match only the range of IPs from 10.20.2.1 to 10.20.2.9, the filter "10.20.2.?" is used.

e. The 'Path' defines the path the BOT monitors. The BOT will only monitor operations on files or directories that reside on the specified path. Only one path supported for each BOT. Wildcards are used (e.g. "\vol\vol0\Users*", this will match with any subdirectory of Users).

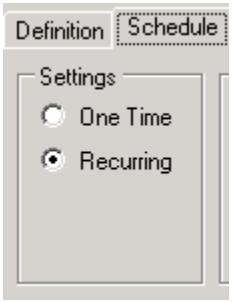
f. The 'File or Directory Name' defines a certain file or directory name to match. Only one file or directory name is allowed. Wildcards are used (e.g., "*Sales*", this will match all folders/files that contains the word Sales within it.)

g. The 'Extension' defines the extension the BOT monitors. The BOT will monitor operations on files with the specified extension. Only one extension is allowed. Wildcards are used (e.g., "mp?" will match with file extensions as mp3 or mp4).

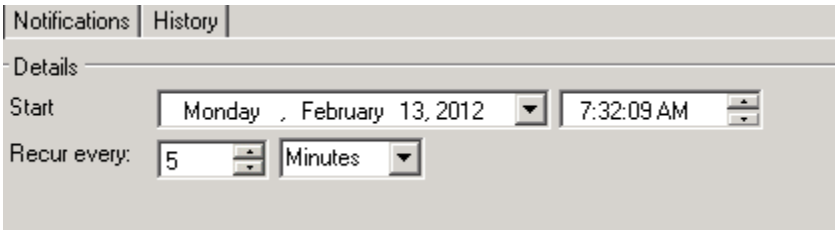
h. Wildcards supported are ('*': Zero or more characters, '?': Exactly one character).

Copyright © 2012 by NTP Software®. All rights reserved.

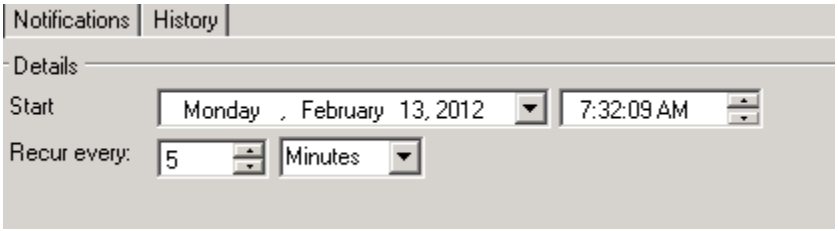
8. On the **Schedule** tab, select whether the BOT is to run only once or recurrently.



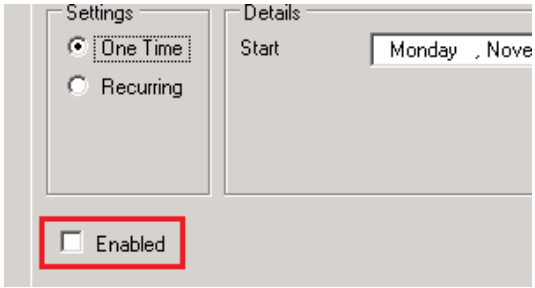
9. Select the BOT start time.



10. If you selected the BOT to be recurring, select how often it should run. When the BOT runs, it will notify the administrator about any behavior that matches the BOT that occurred during the specified time period. The minimum reoccurring time is 5 minutes.

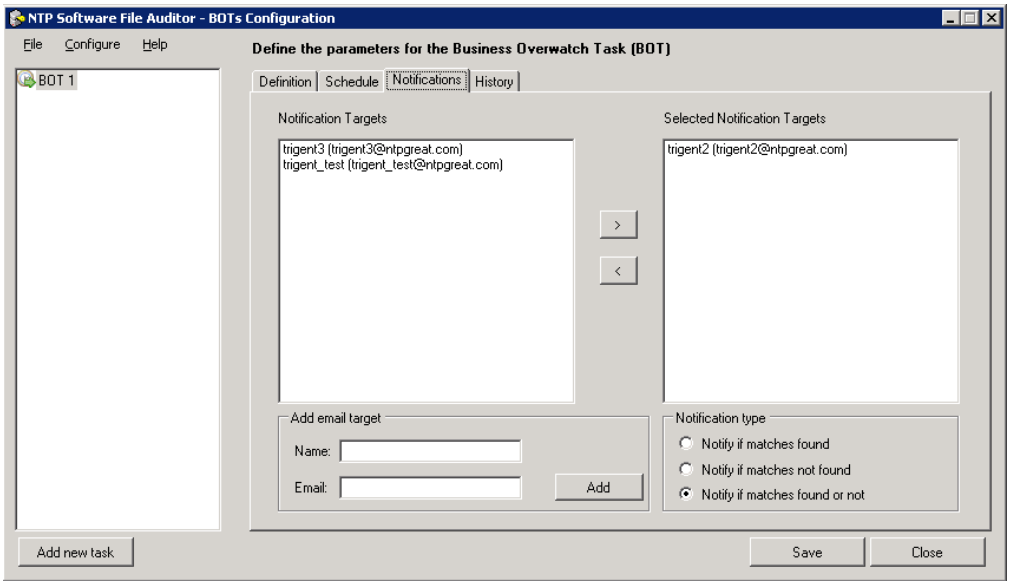


11. You can enable/disable the BOT by checking/un-checking the **Enabled** checkbox. A disabled BOT will not send notification emails or generate history.

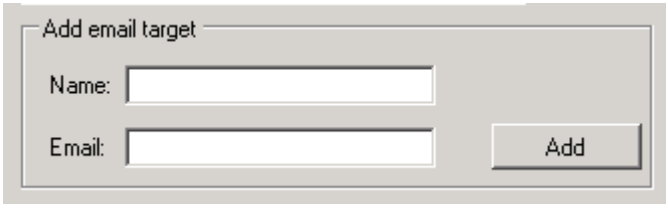


Copyright © 2012 by NTP Software®. All rights reserved.

12. From the **Notifications** tab, specify the email accounts to receive notifications when the BOT runs. The **Selected Notifications Targets** lists the recipients of notifications. The **Potential Notification Targets** lists the available email accounts from which you can select. If you move an email from the **Potential Notification Targets** list to the **Selected Notification Targets** list, the BOT will notify these users.

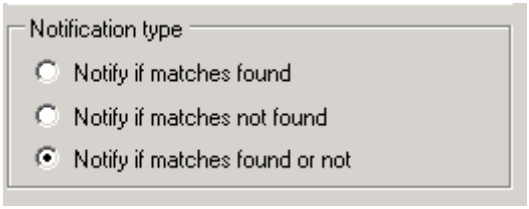


13. You may add email accounts from the **Add Email Target** panel by providing the target name and the email address. Click the **Add** button.



Copyright © 2012 by NTP Software®. All rights reserved.

14. Specify when notifications should be sent.



NOTES:

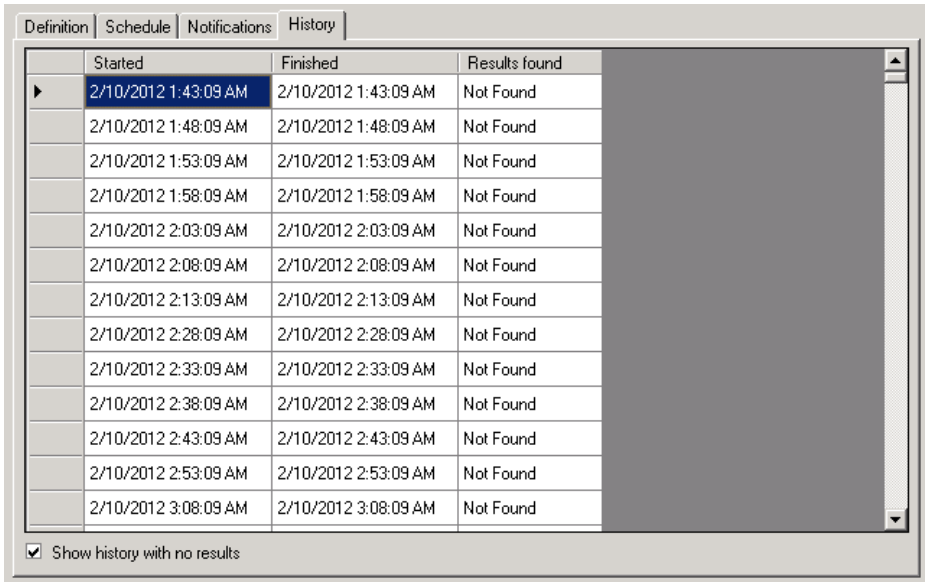
a. The 'Notify if matches found' sends an email notification only if the criteria defined in BOT definition is met.

b. The 'Notify if matches not found' sends an email notification only if the criteria defined in BOT Definition is not met.

c. The 'Notify if matches found or not' sends an email notification every time the BOT executes.

15. Save the BOT after specifying the BOT criteria. You must save the changes before selecting another BOT from the existing BOTs list otherwise you will lose your changes. You may choose to close at any time.

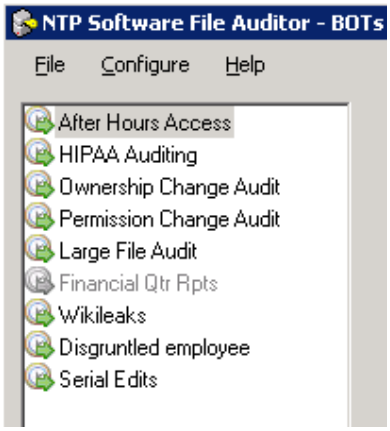
16. Use the **History** tab to check the scans done along with the matches that the BOT found with the File Auditor database, if any.



Copyright © 2012 by NTP Software®. All rights reserved.

Default BOTs

File Auditor BOTs ship with a set of default BOTs; they provide examples of how File Auditor BOTs are used. The user can also edit the default BOTs to satisfy his needs.



1. After Hours Access: This BOT is used to discover any operations done after hours. It runs every day (by default, at 8 am) and analyzes the data of the previous 14 hours to see if someone performed any operations. For best results, this BOT should be set to run every day at the start of the working day.
2. HIPAA Auditing: This BOT discovers any suspicious behavior done to the folder that contains health information. This ensures compliance with the Health Insurance Portability and Accountability Act (HIPAA). This BOT runs every 30 minutes and notifies you if someone read/edited these private documents in the past hour.
3. Ownership Change Audit: This BOT notifies you when a user takes ownership of a file or changes the owner of a file. Make sure to specify the path to monitor.
4. Permission Change Audit: This BOT notifies you when a user changes the security of a file or a directory.
5. Large File Audit: This BOT notifies you when a user creates any file larger than 500MB in a specific directory.
6. Financial Qtr Rpts: This BOT is used for financial quarterly reports to discover all modifications done to the financial reports directory by any user in the last quarter.
7. Wikileaks: This BOT discovers problems similar to the Wikileaks problem. It will discover whether any user has performed a large number of file copies/downloads in the last 30 minutes.
8. Disgruntled Employee: This BOT discovers whether any user has deleted a large number of files in the last hour.
9. Serial Edits: This BOT discovers whether any user has edited many files in the last hour.

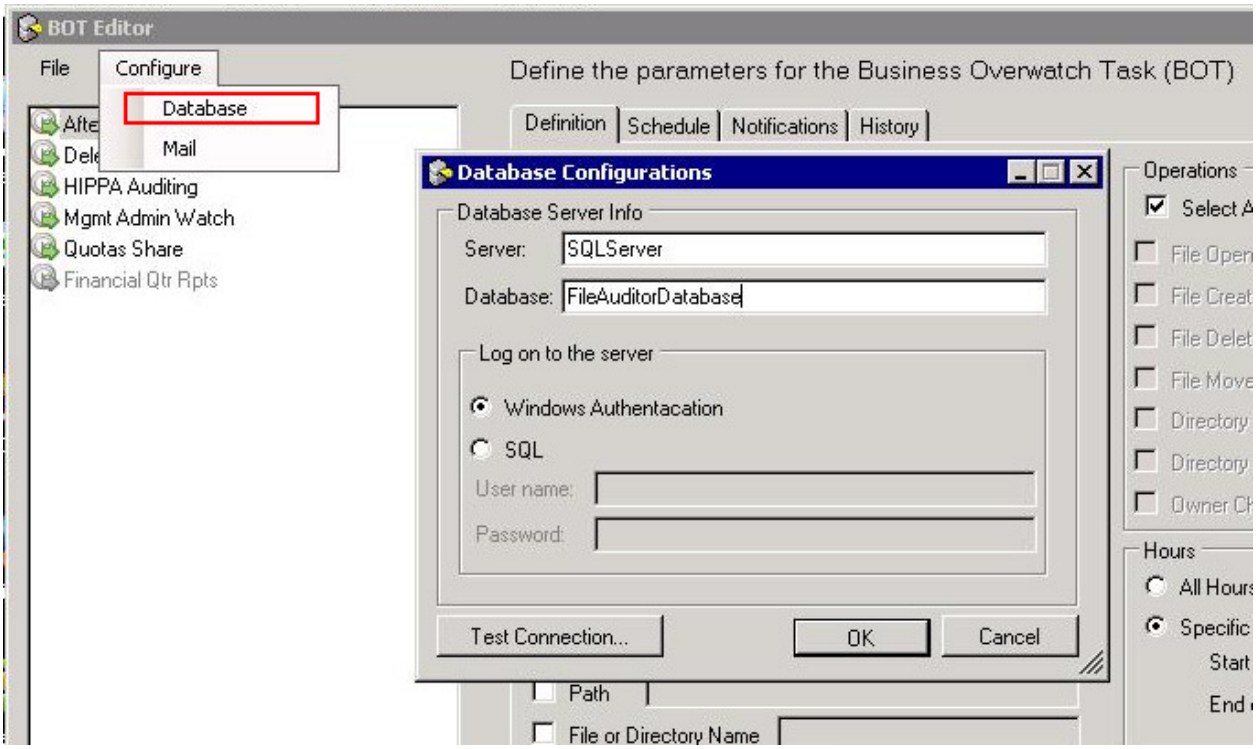
Copyright © 2012 by NTP Software®. All rights reserved.

File Auditor Database and Email Settings

File Auditor Business Overwatch Tasks scan the File Auditor database and send email notifications once they finds the pattern you defined for a task. This section shows how to point File Auditor BOTs to a certain File Auditor database and how to add your email server configurations.

Database Settings

Once the BOT editor starts, it will load all the BOTs defined in the database that you entered during installing File Auditor. You can also point the BOT Editor to a different database.



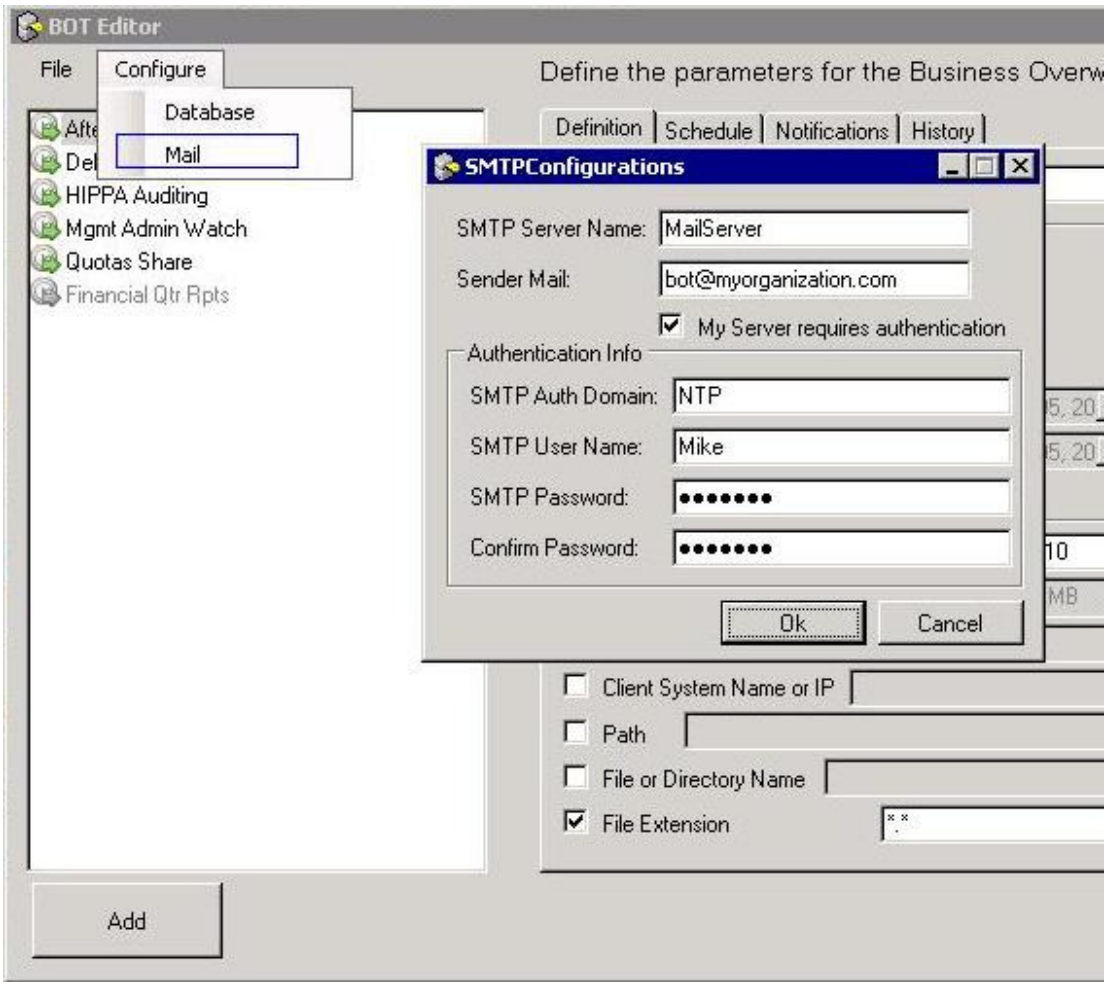
Copyright © 2012 by NTP Software®. All rights reserved.

Email Configuration

You can configure the email server that File Auditor BOTs should use to send notification emails. BOTs support the following SMTP authentication methods:

1. Anonymous.
2. Integrated Windows Authentication (NTLM).

Select **My Server requires authentication** to enable Integrated Windows authentication as shown below. Anonymous authentication is the default option.



Copyright © 2012 by NTP Software®. All rights reserved.

File Auditor BOTs Demo Mode

Initially, your File Auditor database is empty and does not contain any suspicious user operations about which File Auditor BOTs should notify you. For Demo purposes, you can enable Demo mode, which will make BOT editor use a demo database installed with File Auditor, this database contains pre-configured BOTs and actions that will send demo emails to your inbox.

In order to use the Demo mode, please perform the following:

1. Enable Demo Mode; go to Windows Registry Editor and go to the key (HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\File Auditor\Bot) and change the value **DemoModeOn** to **1.**
2. Restart the service and the BOT interface.
3. You will notice some BOTs defined in the BOT editor:
    - After Hours Access
    - HIPAA Auditing
    - Mgmt Admin Watch
    - Quota Share
    - Financial Qtr Rpts
    - Wikileaks
    - Disgruntled employee
    - Serial Edits
4. Open the BOT Editor and configure your email settings. Please refer to the Email Configuration section.
5. Add your email to the Selected Targets list in the Notification settings for each BOT (at least one). Please refer to How to Define a BOT.
6. Check your Inbox; you should find an email from the BOT service, listing some demo operations.

Copyright © 2012 by NTP Software®. All rights reserved.

NTP Software Smart Policy Manager

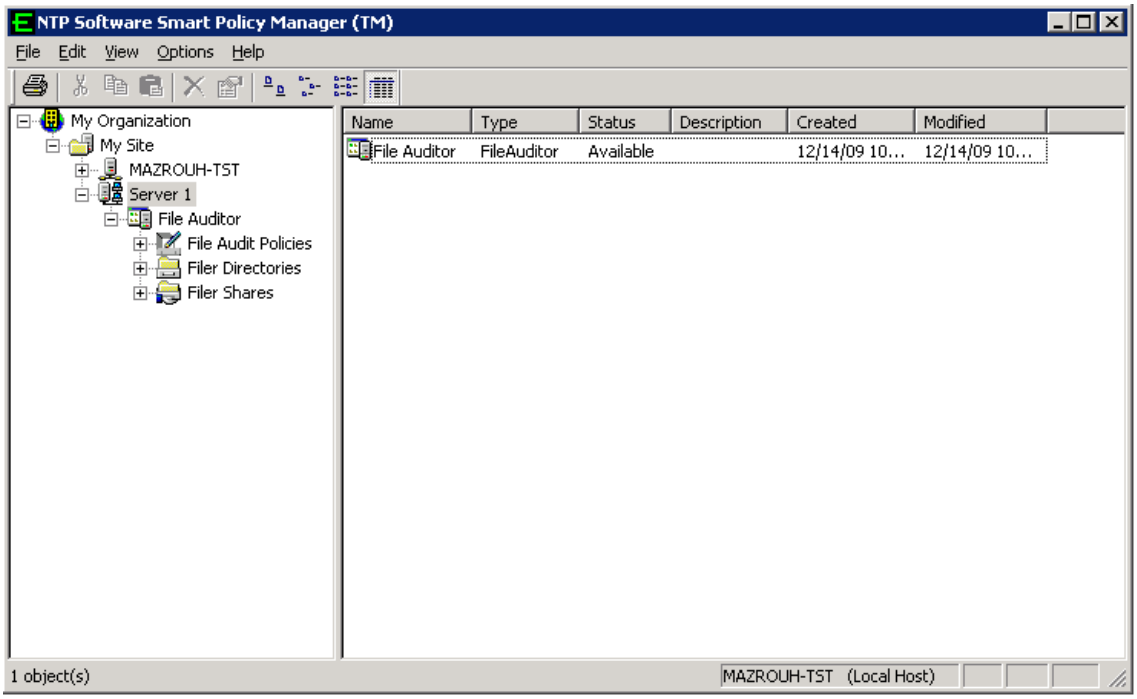
NTP Software Smart Policy Manager Overview

The first step in using NTP Software File Auditor is to lay out your strategy for managing users' file and directory operations. Before doing this, though, let us look at our underlying policy-based rules engine: NTP Software Smart Policy Manager™.

NTP Software Smart Policy Manager allows you to monitor your users' file and directory operations in a way that is a unique fit to your organization. If you manage by geography or administrative unit, you can use that plan. If you manage by class of machine, that approach works just as well. Often, companies use a mixed mode—perhaps geography, a department, and a machine type. NTP Software Smart Policy Manager has the flexibility you need to make using NTP Software File Auditor simple.

Once you have laid out your management structure, NTP Software Smart Policy Manager provides policy replication throughout your enterprise. It allows machines to access the policies in their containers and inherit policies from all levels above that point in your hierarchy. You no longer need to configure and manage the machines on your network one by one.

As you start to configure the software you have installed, begin with the top-level container under the root organization (in the following example, *My Site*). This is the Global Network configuration, whose container is created during installation.



Copyright © 2012 by NTP Software®. All rights reserved.

Managing the NTP Software File Auditor Service through an NTP Software File Auditor Admin Client Running on a Different Machine

This section provides step-by-step instructions for installing the NTP Software File Auditor Admin Client, enabling you to administer the NTP Software File Auditor service running on a different machine. This kind of NTP Software File Auditor Admin Client installation enables NTP Software File Auditor administrators to administer NTP Software File Auditor easily when it is installed on all the servers over the entire network. This can be done through a local user interface that is easily installed on the administrator's local machine.

For an NTP Software File Auditor administrator to be able to use the NTP Software File Auditor Admin Client, the NTP Software Smart Policy Manager Admin and NTP Software File Auditor Admin components should be installed on the administrator's local machine per the following instructions.

IMPORTANT NOTES

There is a slight difference in the installation of NTP Software Smart Policy Manager and NTP Software File Auditor on an NTP Software File Auditor Server versus the installation on an administrator's local machine.

NTP Software File Auditor Admin Client User Interface is using RPC to communicate to the NTP Software Smart Policy Manager service. Therefore, NTP Software File Auditor Administrator needs to have permissions to run and execute RPC on the managed machine. A standard user does not have RPC Permission by default. Thus, if the user performing the administration is not an administrator in the domain, the user needs to be added to the Distributed COM Users group on the machine to be managed.

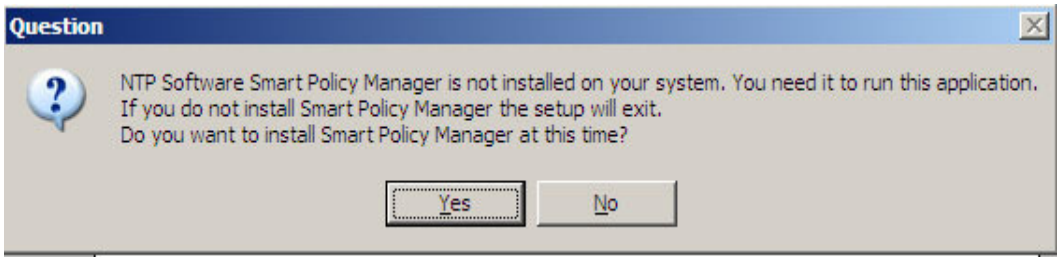
Copyright © 2012 by NTP Software®. All rights reserved.

Installing the NTP Software Smart Policy Manager Admin Component

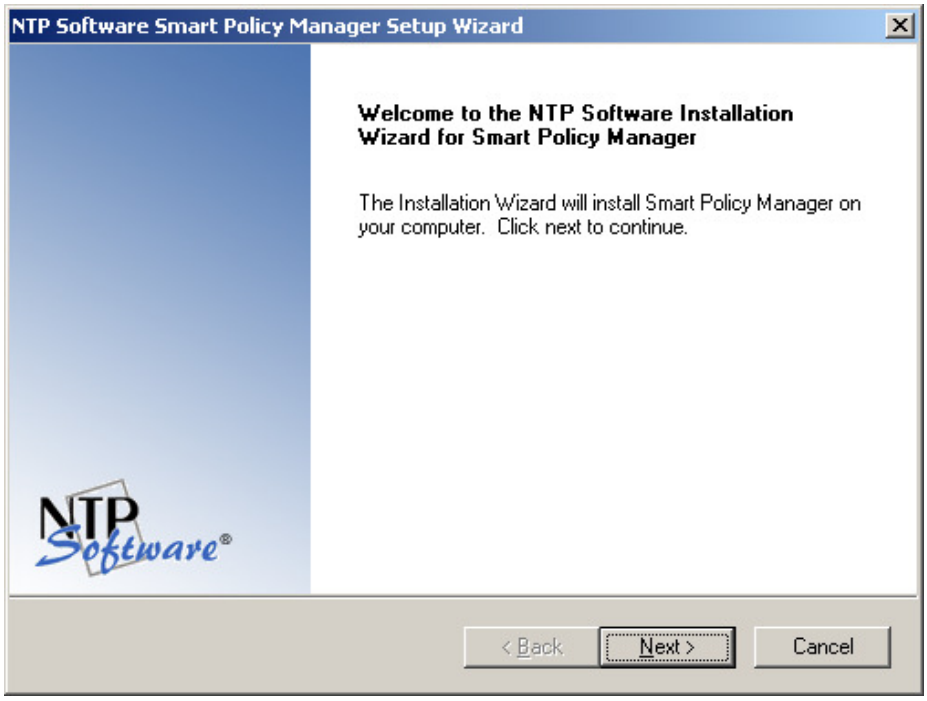
1. Log on to your local computer using an account with administrator privileges.

2. On the NTP Software Product Installation page, click your product installation link under the **Product Components** section.

3. When prompted to install NTP Software Smart Policy Manager, click **Yes** to launch the Installation Wizard.

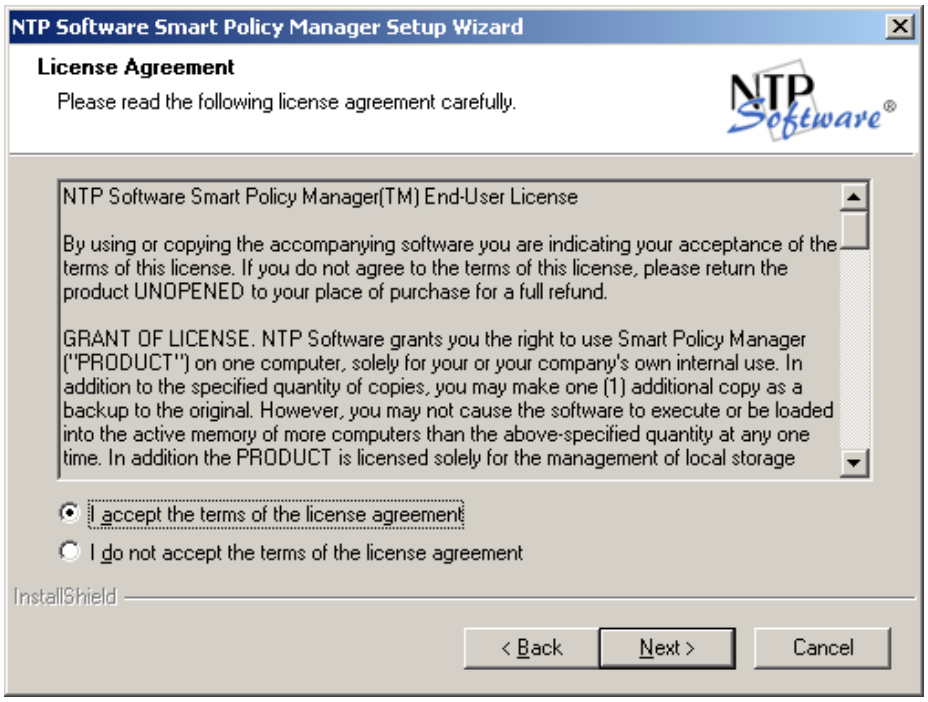

Question
NTP Software Smart Policy Manager is not installed on your system. You need it to run this application.
If you do not install Smart Policy Manager the setup will exit.
Do you want to install Smart Policy Manager at this time?
Yes
No

4. In the NTP Software Smart Policy Manager installation welcome dialog box, click **Next**.

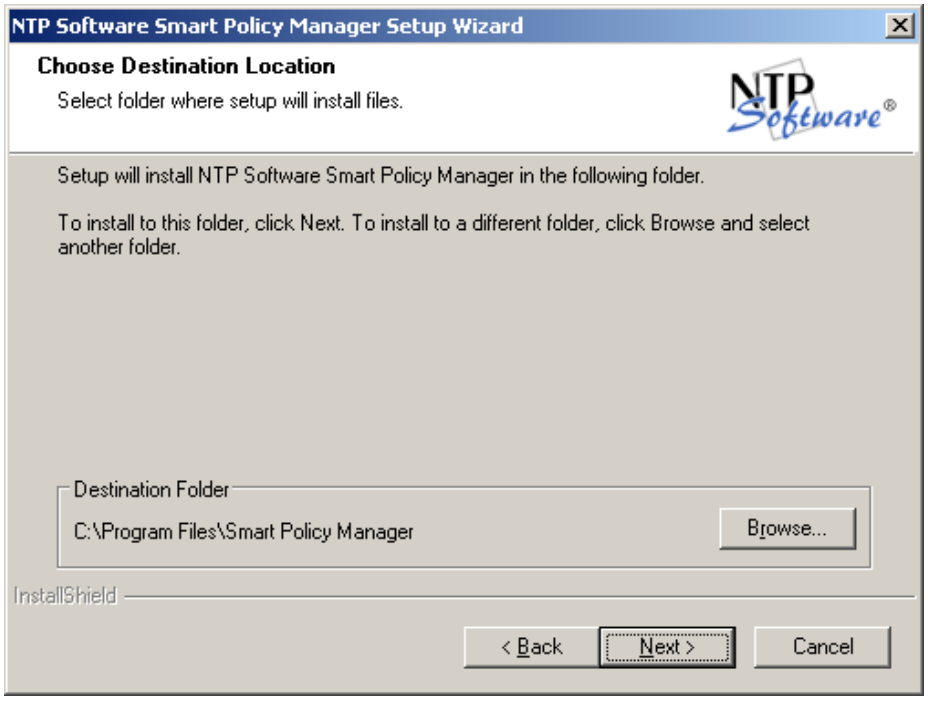

NTP Software Smart Policy Manager Setup Wizard
Welcome to the NTP Software Installation Wizard for Smart Policy Manager
The Installation Wizard will install Smart Policy Manager on your computer. Click next to continue.
NTP Software®
< Back
Next >
Cancel

Copyright © 2012 by NTP Software®. All rights reserved.

5. Select **I accept the terms of the license agreement** in the License Agreement dialog box and then click **Next**.

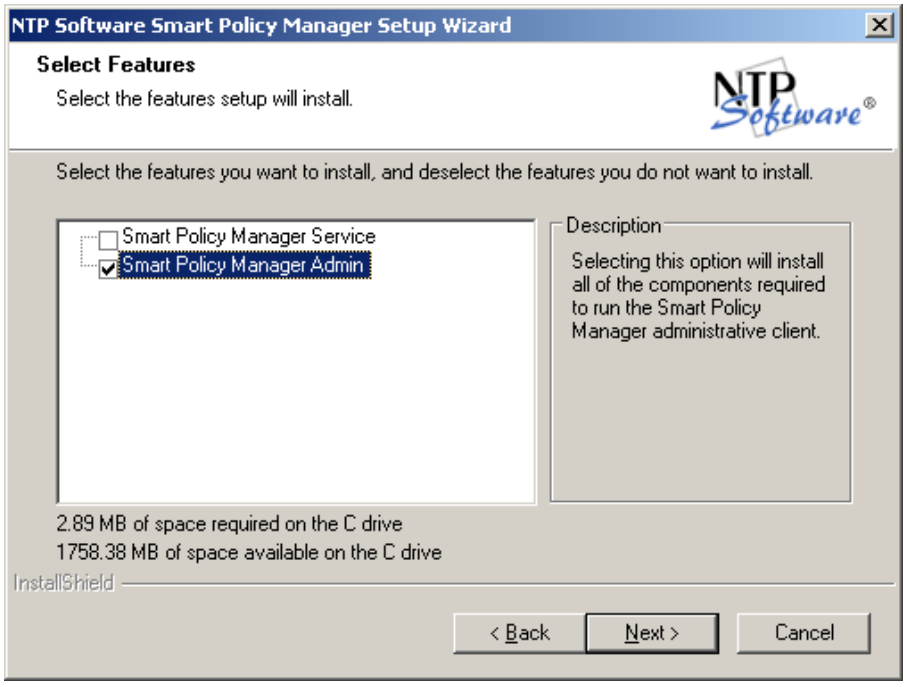

NTP Software Smart Policy Manager Setup Wizard
License Agreement
Please read the following license agreement carefully.
NTP Software
NTP Software Smart Policy Manager(TM) End-User License
By using or copying the accompanying software you are indicating your acceptance of the terms of this license. If you do not agree to the terms of this license, please return the product UNOPENED to your place of purchase for a full refund.
GRANT OF LICENSE. NTP Software grants you the right to use Smart Policy Manager ("PRODUCT") on one computer, solely for your or your company's own internal use. In addition to the specified quantity of copies, you may make one (1) additional copy as a backup to the original. However, you may not cause the software to execute or be loaded into the active memory of more computers than the above-specified quantity at any one time. In addition the PRODUCT is licensed solely for the management of local storage
I accept the terms of the license agreement
I do not accept the terms of the license agreement
InstallShield
< Back
Next >
Cancel

6. In the **Choose Destination Location** dialog box, browse to the needed location and then click **Next**.

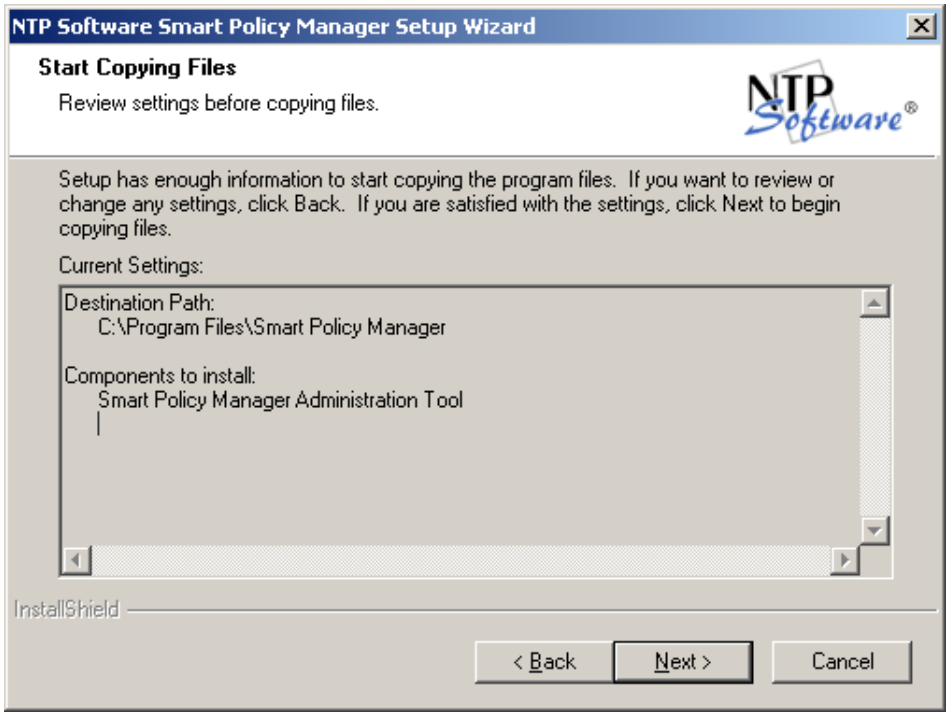

NTP Software Smart Policy Manager Setup Wizard
Choose Destination Location
Select folder where setup will install files.
NTP Software
Setup will install NTP Software Smart Policy Manager in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\Smart Policy Manager
Browse...
InstallShield
< Back
Next >
Cancel

Copyright © 2012 by NTP Software®. All rights reserved.

7. Select only the **Smart Policy Manager Admin** component in the **Select Features** dialog box. Click **Next**.

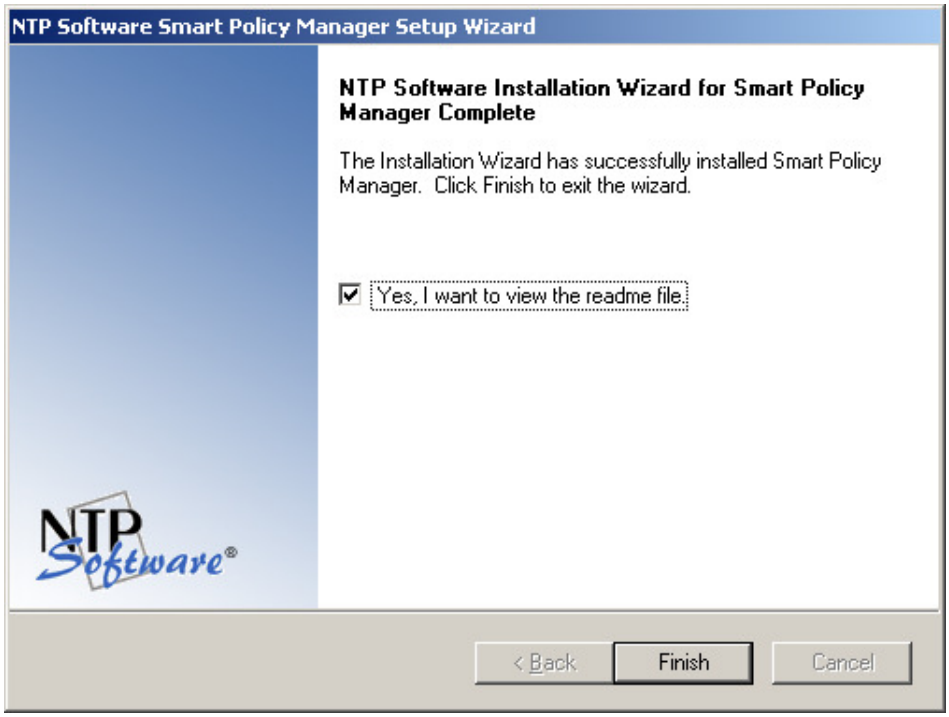

NTP Software Smart Policy Manager Setup Wizard
Select Features
Select the features setup will install.
NTP Software
Select the features you want to install, and deselect the features you do not want to install.
Smart Policy Manager Service
Smart Policy Manager Admin
Description
Selecting this option will install all of the components required to run the Smart Policy Manager administrative client.
2.89 MB of space required on the C drive
1758.38 MB of space available on the C drive
InstallShield
< Back
Next >
Cancel

8. The **Start Copying Files** dialog box prompts you to begin copying files.


NTP Software Smart Policy Manager Setup Wizard
Start Copying Files
Review settings before copying files.
NTP Software
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Destination Path:
C:\Program Files\Smart Policy Manager
Components to install:
Smart Policy Manager Administration Tool
InstallShield
< Back
Next >
Cancel

Copyright © 2012 by NTP Software®. All rights reserved.

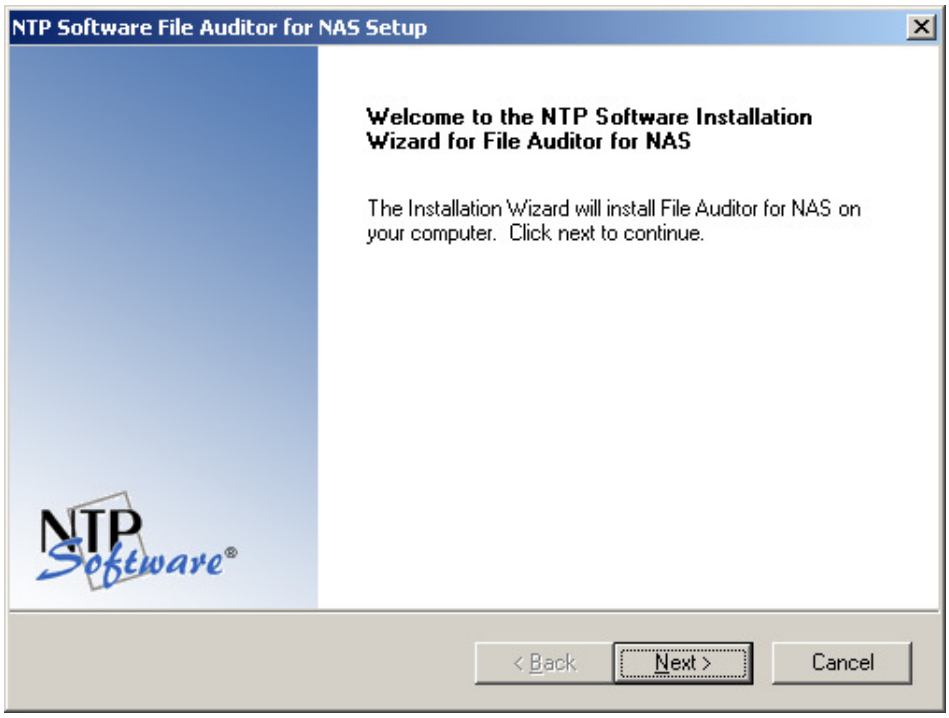
9. When the file installation is complete, a dialog box offers you the opportunity to view the readme file, which may contain documentation updates and other items. If you *do not* want to view the readme file at this time, clear the option **Yes, I want to view the readme file**. Click **Finish**.


NTP Software Smart Policy Manager Setup Wizard
NTP Software Installation Wizard for Smart Policy Manager Complete
The Installation Wizard has successfully installed Smart Policy Manager. Click Finish to exit the wizard.
Yes, I want to view the readme file.
NTP Software®
< Back
Finish
Cancel

Copyright © 2012 by NTP Software®. All rights reserved.

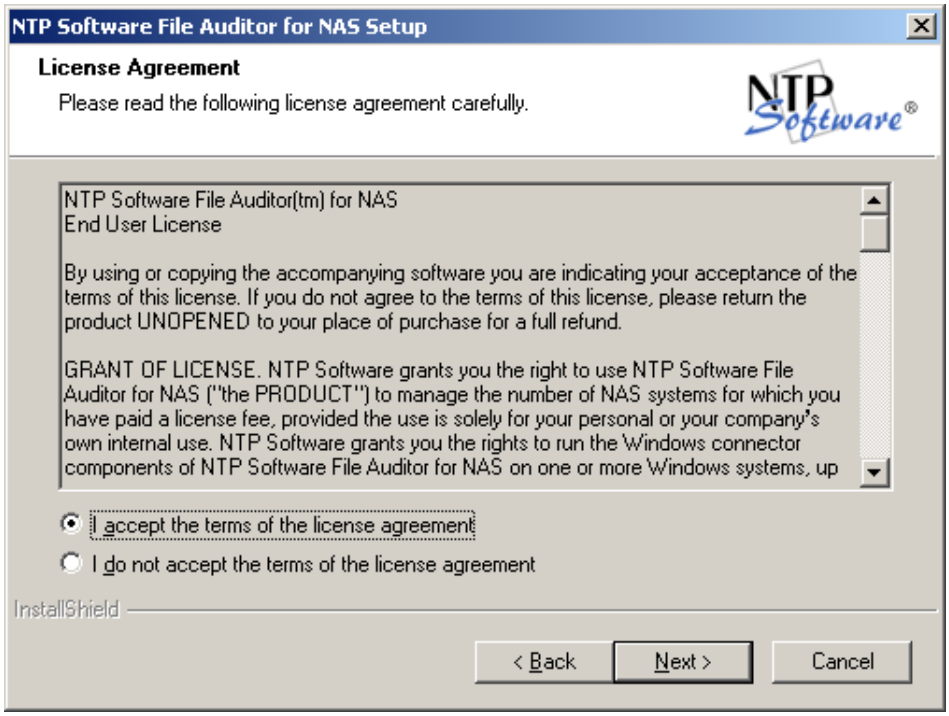
Installing the NTP Software File Auditor Admin Component

1. The NTP Software File Auditor welcome dialog box pops up automatically. Click **Next** to continue.


NTP Software File Auditor for NAS Setup
Welcome to the NTP Software Installation Wizard for File Auditor for NAS
The Installation Wizard will install File Auditor for NAS on your computer. Click next to continue.
NTP Software®
< Back
Next >
Cancel

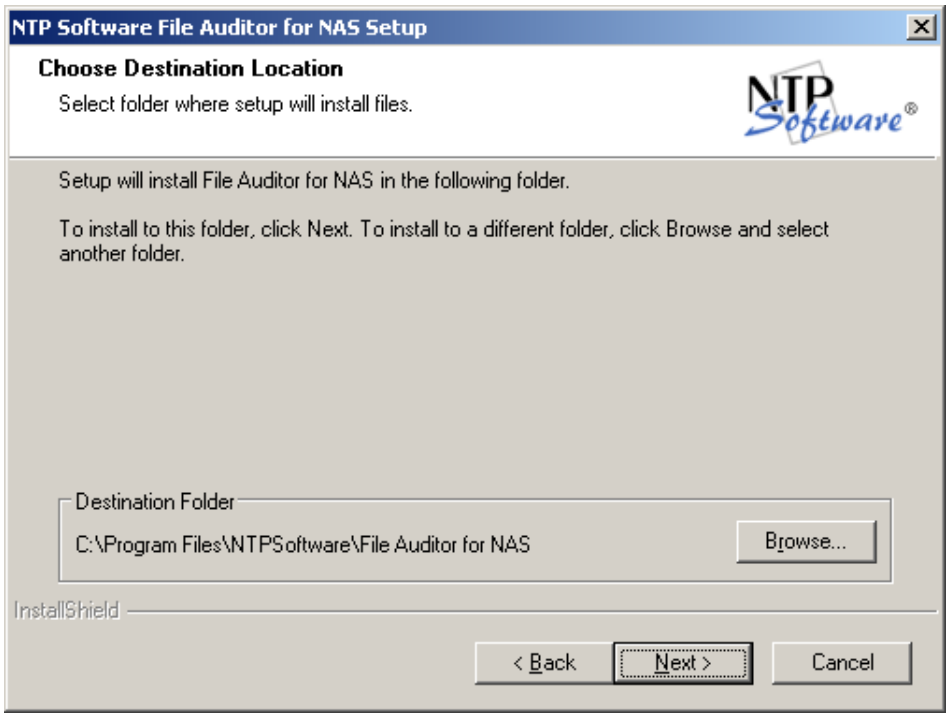
Copyright © 2012 by NTP Software®. All rights reserved.

2. In the **License Agreement** dialog box, select **I accept the terms of the license agreement** and then click **Next**.


NTP Software File Auditor for NAS Setup
License Agreement
Please read the following license agreement carefully.
NTP Software
NTP Software File Auditor(tm) for NAS
End User License
By using or copying the accompanying software you are indicating your acceptance of the terms of this license. If you do not agree to the terms of this license, please return the product UNOPENED to your place of purchase for a full refund.
GRANT OF LICENSE. NTP Software grants you the right to use NTP Software File Auditor for NAS ("the PRODUCT") to manage the number of NAS systems for which you have paid a license fee, provided the use is solely for your personal or your company's own internal use. NTP Software grants you the rights to run the Windows connector components of NTP Software File Auditor for NAS on one or more Windows systems, up
I accept the terms of the license agreement
I do not accept the terms of the license agreement
InstallShield
< Back
Next >
Cancel

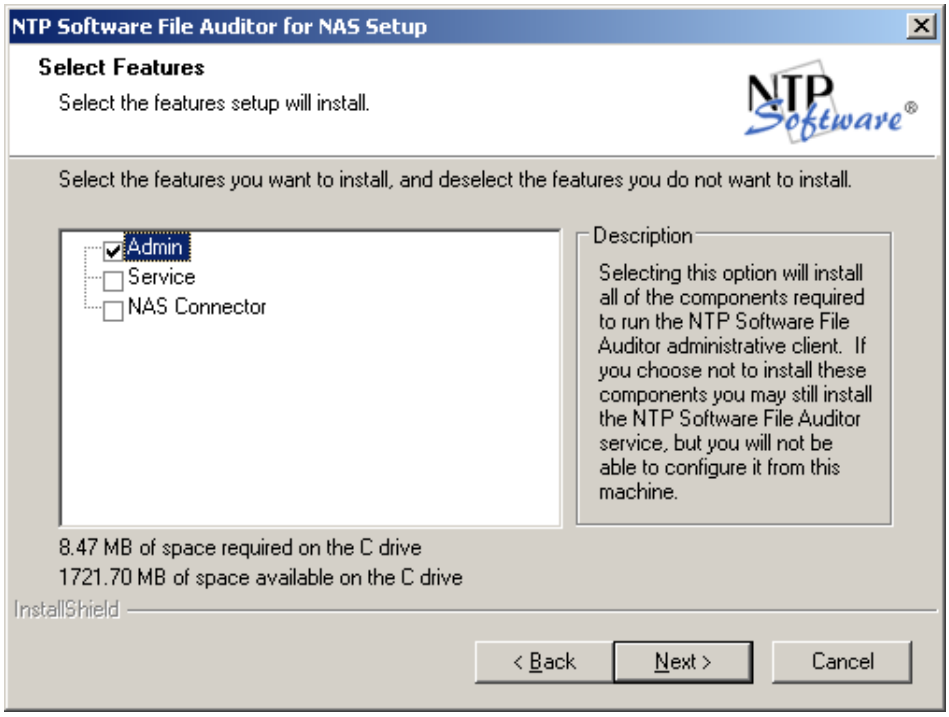
Copyright © 2012 by NTP Software®. All rights reserved.

3. In the **Choose Destination Location** dialog box, browse to the desired destination, or click **Next** if the default destination location is appropriate.


NTP Software File Auditor for NAS Setup
Choose Destination Location
Select folder where setup will install files.
NTP Software®
Setup will install File Auditor for NAS in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\NTPSoftware\File Auditor for NAS
Browse...
InstallShield
< Back
Next >
Cancel

Copyright © 2012 by NTP Software®. All rights reserved.

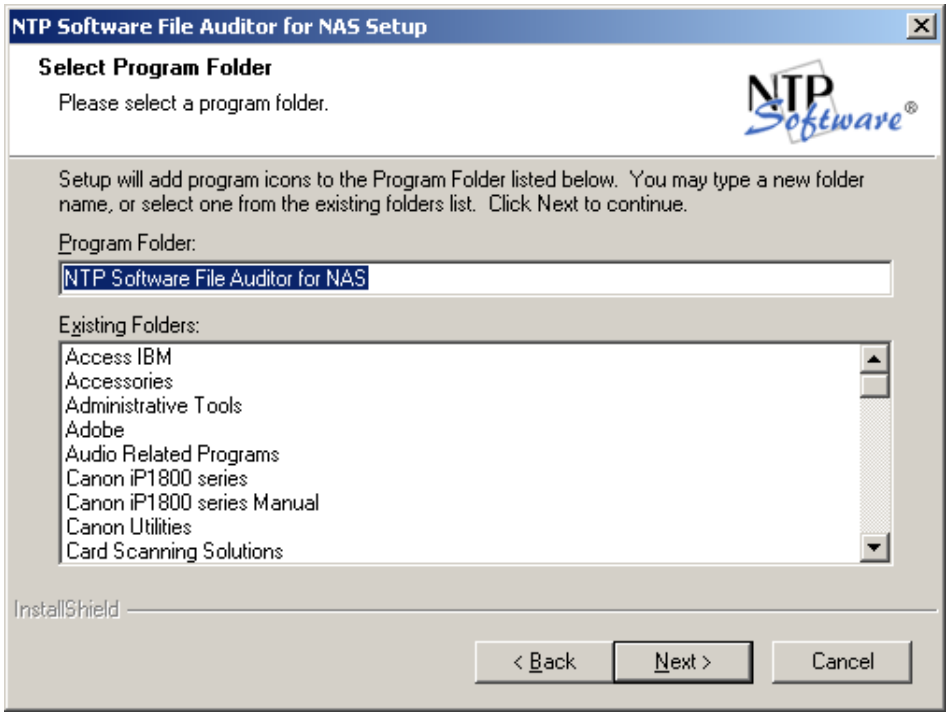
4. In the **Select Features** dialog box, make sure that only the **Admin** component is selected and then click **Next**.


NTP Software File Auditor for NAS Setup
Select Features
Select the features setup will install.
NTP Software®
Select the features you want to install, and deselect the features you do not want to install.
Admin
Service
NAS Connector
Description
Selecting this option will install all of the components required to run the NTP Software File Auditor administrative client. If you choose not to install these components you may still install the NTP Software File Auditor service, but you will not be able to configure it from this machine.
8.47 MB of space required on the C drive
1721.70 MB of space available on the C drive
InstallShield
< Back
Next >
Cancel

IMPORTANT: Because we only need the Admin User Interface to manage and configure the policies, we checked the Admin Client only. We are not seeking a full NTP Software File Auditor installation.

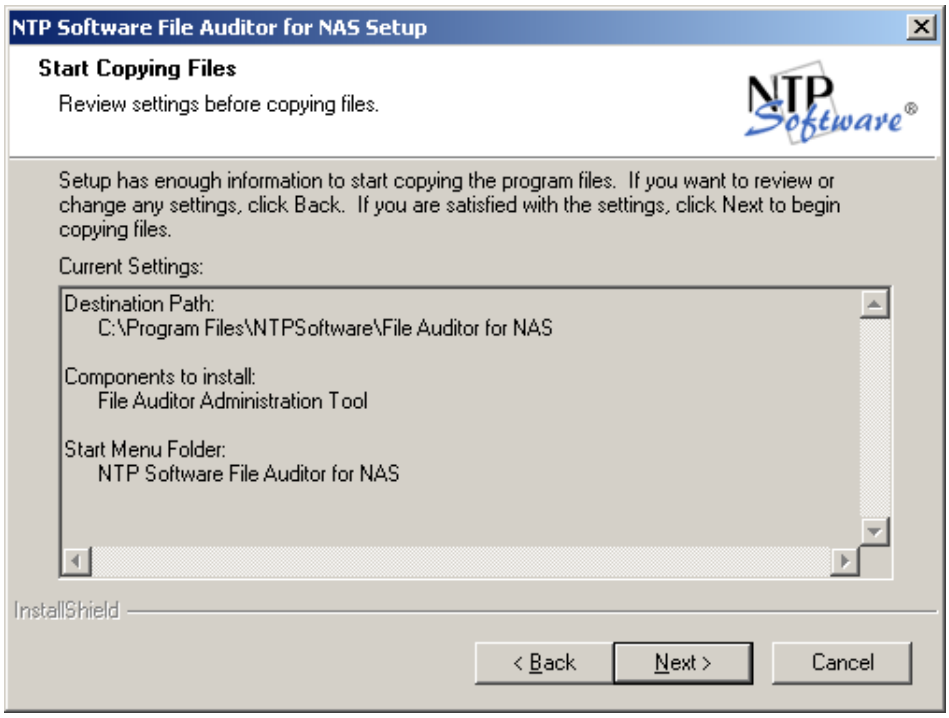
Copyright © 2012 by NTP Software®. All rights reserved.

5. Specify the program folder (using the default program folder is recommended) and click **Next**. The setup program adds program icons to the program folder.


NTP Software File Auditor for NAS Setup
Select Program Folder
Please select a program folder.
NTP Software®
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.
Program Folder:
NTP Software File Auditor for NAS
Existing Folders:
Access IBM
Accessories
Administrative Tools
Adobe
Audio Related Programs
Canon iP1800 series
Canon iP1800 series Manual
Canon Utilities
Card Scanning Solutions
InstallShield
< Back
Next >
Cancel

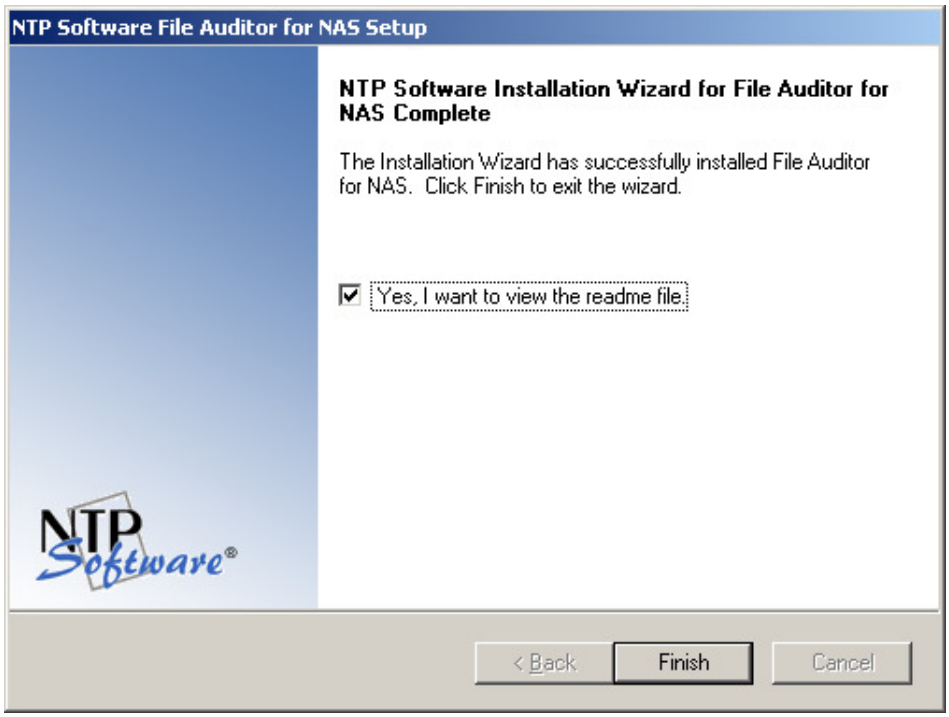
Copyright © 2012 by NTP Software®. All rights reserved.

6. Click **Next** when the **Start Copying Files** dialog box appears (assuming that the destination paths are correct). NTP Software File Auditor setup begins transferring files to the specified locations.


NTP Software File Auditor for NAS Setup
Start Copying Files
Review settings before copying files.
NTP Software®
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Destination Path:
C:\Program Files\NTPSoftware\File Auditor for NAS
Components to install:
File Auditor Administration Tool
Start Menu Folder:
NTP Software File Auditor for NAS
InstallShield
< Back
Next >
Cancel

Copyright © 2012 by NTP Software®. All rights reserved.

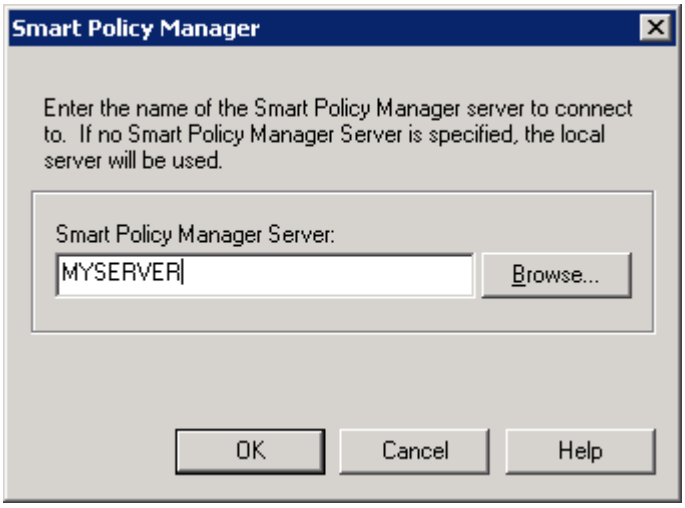
7. When the file installation is complete, a dialog box offers you the opportunity to view the readme file. If you *do not* want to view the readme file at this time, clear the option **Yes, I want to view the readme file**. Click **Finish**. With this step, NTP Software File Auditor installation is completed.


NTP Software File Auditor for NAS Setup
NTP Software Installation Wizard for File Auditor for NAS Complete
The Installation Wizard has successfully installed File Auditor for NAS. Click Finish to exit the wizard.
Yes, I want to view the readme file.
NTP Software®
< Back
Finish
Cancel

Copyright © 2012 by NTP Software®. All rights reserved.

Administering NTP Software File Auditor through an NTP Software File Auditor Admin Client Running on a Different Machine.

1. Click **Start > Programs > NTP Software File Auditor > NTP Software File Auditor Admin**.
2. In the **Smart Policy Manager** dialog box, specify the Smart Policy Manager Server to which you want to connect.


Smart Policy Manager
Enter the name of the Smart Policy Manager server to connect to. If no Smart Policy Manager Server is specified, the local server will be used.
Smart Policy Manager Server:
MYSERVER
Browse...
OK
Cancel
Help

NOTE: The Smart Policy Manager Admin component is installed on the local machine, so there is no Smart Policy Manager service installed. Thus, NTP Software File Auditor cannot talk to the local Smart Policy Manager service because it does not exist, so we specify the Smart Policy Manager service with which NTP Software File Auditor should communicate.

In very large organizations, you may have offices all over the world. Make sure you connect to the server(s) at a reasonable distance to maintain good speed.

As shown, the NTP Software File Auditor Admin Client User interface is displayed with **MYSERVER** as a node in the left menu tree and all the NTP Software File Auditor policy details.

To connect to more than one Smart Policy Manager service at the same time, click **File > Active Server** and then insert the server name or the server IP address. This allows you to add all the servers on your entire network administer them as needed.

Copyright © 2012 by NTP Software®. All rights reserved.

Installing File Auditor in Clustered Environments

NOTES:

- NTP Software File Auditor requires a manual setup by an administrator for clustered environments.
- Although the Connector service can be started on the servers on which NTP Software File Auditor was installed, in the NTP Software File Auditor user interface, the Filer, Celerra, or EVS is assigned to only one server node and must be reassigned manually from a previously assigned node.
- A Filer, Celerra, or EVS cannot communicate with more than one NTP Software File Auditor server at a time.

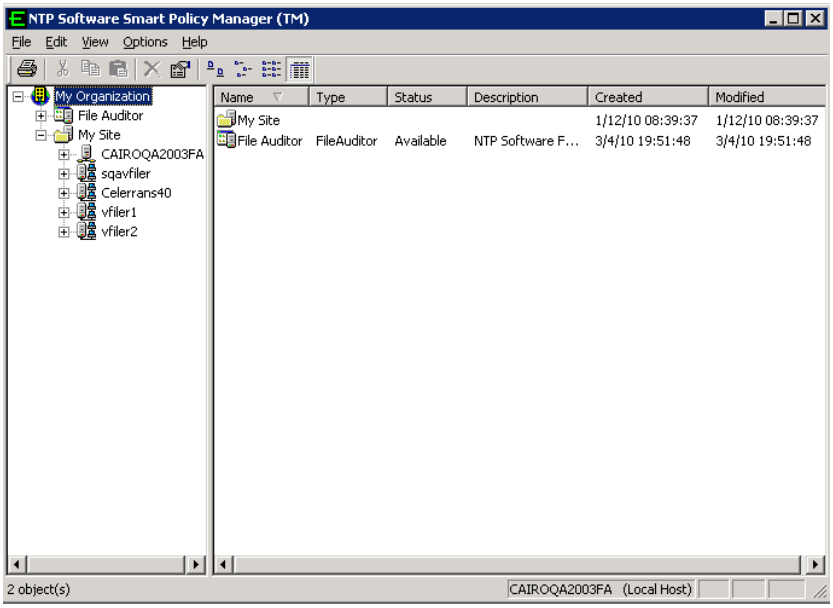
Copyright © 2012 by NTP Software®. All rights reserved.

Installing the NTP Software File Auditor in Clustered Environments

To install NTP Software File Auditor in a clustered environment, apply the following steps:

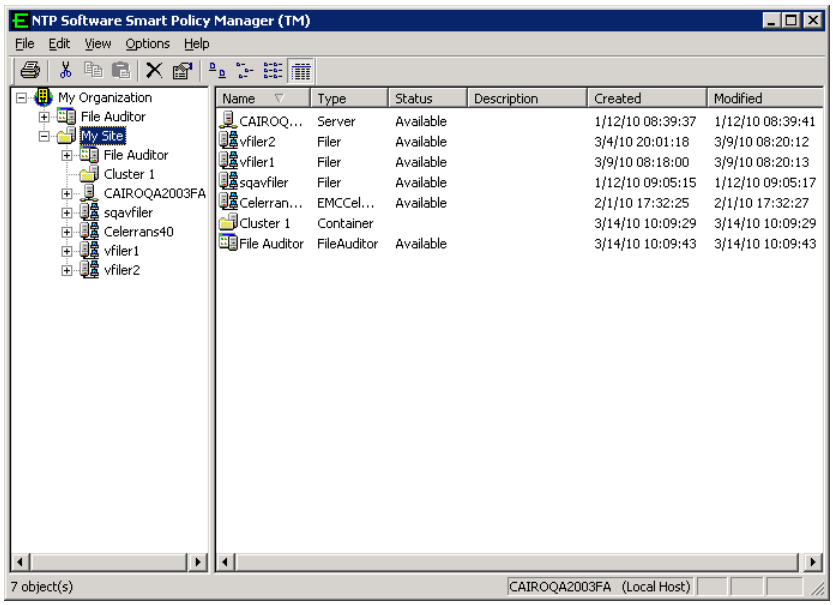
1. Install NTP Software File Auditor on a server, as described in NTP Software File Auditor installation guides.
2. After NTP Software File Auditor is installed successfully, open NTP Software File Auditor to find the global container (**My Organization** in this example) at the top of the hierarchy. Click the plus sign (**+**) to expand the container.
3. Click the plus sign (**+**) to expand your site container (**My Site** in this example) in the second tier of the hierarchy.

   Notice the installation server (**Primary Server** in this example) in the third tier of the hierarchy. The NTP Software File Auditor application is also in the third tier.



Copyright © 2012 by NTP Software®. All rights reserved.

4. Right-click the site container (**My Site** in this example) and then select **New > Container** from the pop-up menu to create your cluster container. Give the new container the name of the cluster. In the example, we have used **Cluster 1** as the name.

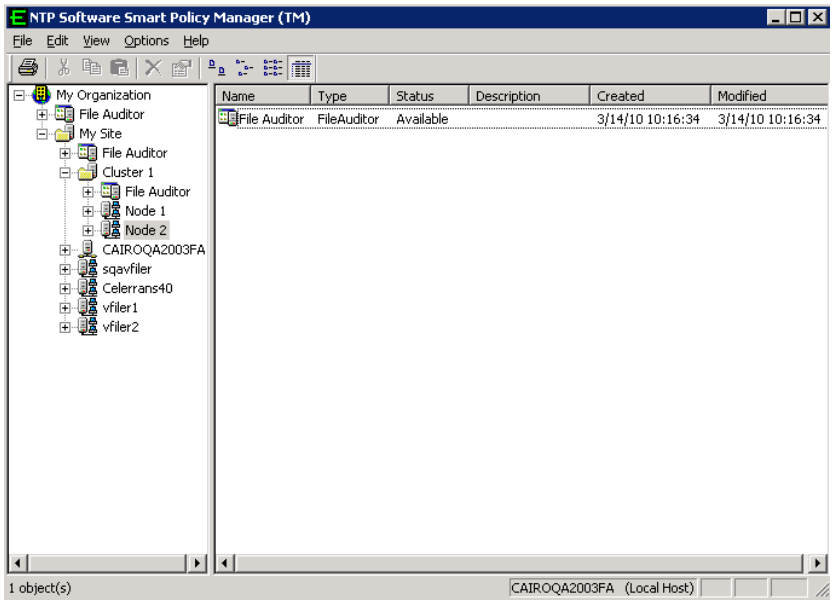

NTP Software Smart Policy Manager (TM)
File Edit View Options Help
My Organization
File Auditor
My Site
File Auditor
Cluster 1
CAIROQA2003FA
sqavfiler
Celerrans40
vfiler1
vfiler2
Name Type Status Description Created Modified
CAIROQ... Server Available 1/12/10 08:39:37 1/12/10 08:39:41
vfiler2 Filer Available 3/4/10 20:01:18 3/9/10 08:20:12
vfiler1 Filer Available 3/9/10 08:18:00 3/9/10 08:20:13
sqavfiler Filer Available 1/12/10 09:05:15 1/12/10 09:05:17
Celerran... EMCCel... Available 2/1/10 17:32:25 2/1/10 17:32:27
Cluster 1 Container 3/14/10 10:09:29 3/14/10 10:09:29
File Auditor FileAuditor Available 3/14/10 10:09:43 3/14/10 10:09:43
7 object(s)
CAIROQA2003FA (Local Host)

5. Right-click the cluster container (**Cluster 1** in this example) and select **New** > **NTP Software File Auditor** from the pop-up menu.

   It is necessary to install NTP Software File Auditor manually on each server you want to add to the tree (**Node 1** and **Node 2** in this example). Choose the option **Adding to an enterprise installation** during the local NTP Software Smart Policy Manager installation on each node and point to the first NTP Software File Auditor server.

Copyright © 2012 by NTP Software®. All rights reserved.

6. Open the cluster container in the NTP Software Smart Policy Manager hierarchy and use the drag-and-drop method to move the nodes into the cluster container. They will appear at the same level as the container File Auditor application, as shown here.



7. Click the plus sign (**+**) next to the NTP Software File Auditor application you have just added to view the global (cluster) policies. Create all policies within this application that will be applied to both nodes. They will be propagated automatically to all nodes within the container.

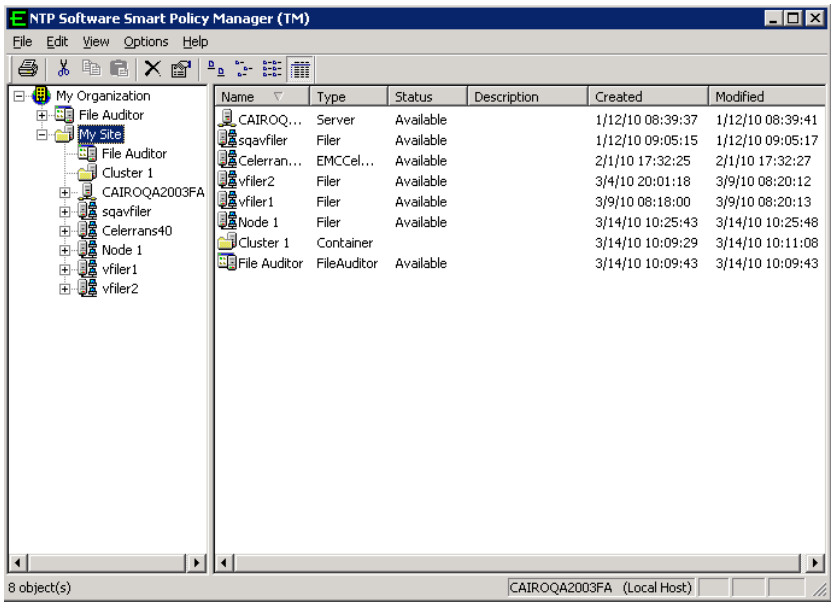
Copyright © 2012 by NTP Software®. All rights reserved.

Installing the NTP Software File Auditor onto a Node Server

This feature enables administrators to group servers, Filers, and Celerras logically to reflect their organizational physical structure, creating policies under a node that can be inherited by all the machines of that node.

To install NTP Software File Auditor onto a node server, apply the following steps:

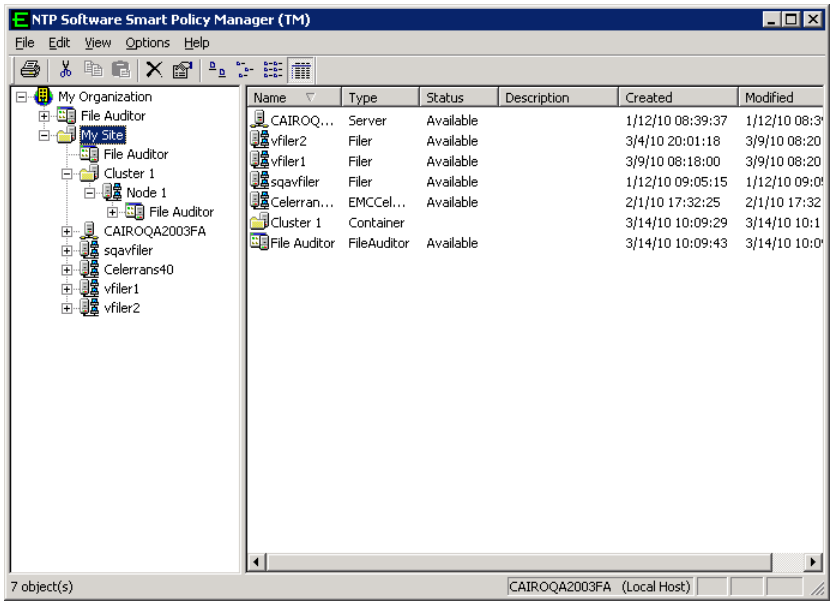
1. It is necessary to install NTP Software File Auditor manually on each of the added nodes (on **Node 1** in this example). Choose the option **Adding to an enterprise installation** during the local NTP Software Smart Policy Manager installation.
2. Right-click the site container and select **New** > **Container** to create a container for the cluster. Give the new container the cluster name.


NTP Software Smart Policy Manager (TM)
File Edit View Options Help
My Organization
File Auditor
My Site
File Auditor
Cluster 1
CAIROQA2003FA
sqavfiler
Celerrans40
Node 1
vfiler1
vfiler2
Name Type Status Description Created Modified
CAIROQ... Server Available 1/12/10 08:39:37 1/12/10 08:39:41
sqavfiler Filer Available 1/12/10 09:05:15 1/12/10 09:05:17
Celerran... EMCCel... Available 2/1/10 17:32:25 2/1/10 17:32:27
vfiler2 Filer Available 3/4/10 20:01:18 3/9/10 08:20:12
vfiler1 Filer Available 3/9/10 08:18:00 3/9/10 08:20:13
Node 1 Filer Available 3/14/10 10:25:43 3/14/10 10:25:48
Cluster 1 Container 3/14/10 10:09:29 3/14/10 10:11:08
File Auditor FileAuditor Available 3/14/10 10:09:43 3/14/10 10:09:43
8 object(s)
CAIROQA2003FA (Local Host)

3. Click the existing server (node) and, while holding down the mouse button, drag and drop the server onto the cluster container to move the server into the cluster hierarchy.
4. Right-click the cluster container and select **New** > **NTP Software File Auditor** from the pop-up menu.

Copyright © 2012 by NTP Software®. All rights reserved.

5. To view the global (cluster) policies, click the plus sign (**+**) next to the NTP Software File Auditor application you have just added.



Create all policies within this application that will be applied to both nodes. They will be propagated down automatically to all nodes within the container.

Copyright © 2012 by NTP Software®. All rights reserved.

Network Attached Storage (NAS) Preparations

Preparing the NetApp Filer

NOTE: Refer to this section only if you have NetApp Filers attached to your environment. *If you do not have NetApp Filers, you should not apply the instructions specified in this section.*

Enabling the fpolicy Management Service (NetApp Filers)

NTP Software File Auditor requires NetApp Filers to run Data ONTAP version 6.5 or later (excluding version 7.1). If your Filer is running a version prior to 6.5, you must upgrade your operating system before you proceed. (Please refer to your Network Appliance documentation for instructions.)

Although NTP Software File Auditor does not install any components on the NetApp Filer, you will need to enable the Data ONTAP fpolicy management service.

For more information on NetApp Filers, consult *NetApp Customer Support Bulletin CSB-0704-02: Fpolicy Update for Data ONTAP*.

Apply the following steps to enable the Data ONTAP fpolicy management service:

1. Log on to the NetApp Filer with an account that has administrative privileges.
2. At the prompt, enter the following command:

   fpolicy create NTPSoftware_FA screen
3. Enter the following command:

   fpolicy enable NTPSoftware_FA
4. To verify that CIFS file policies are now enabled, enter the following command:

   fpolicy show NTPSoftware_FA
5. If you want File Auditor to record Permission and Owner changes for your files and directories, you will need to enable CIFS SetAttr feature of fpolicy, enter the following comand:

   fpolicy options NTPSoftware_FA cifs_setattr on

NOTE: If you don't have any File Audit Policy that monitors *Permission Change* or *Owner Change* events, then you should disable CIFS SetAttr feature.

Copyright © 2012 by NTP Software®. All rights reserved.

These steps create the configuration that allows NTP Software File Auditor to register with and manage your Filer. They must be completed before you try to configure NTP Software File Auditor. Later in this document, a File Auditor policy server with be registered with the Filer. No further Filer administration is required.

NOTES:

- Data ONTAP versions 7.0.6 and 7.2.2 contain a number of fixes that address stability and memory issues related to fpolicy functionality in Data ONTAP. For NetApp Filers, NetApp strongly recommends that customers using fpolicy move to one of these Data ONTAP versions or later (excluding version 7.1).
- The Data ONTAP 7.1 release family is currently not supported with fpolicy.

Copyright © 2012 by NTP Software®. All rights reserved.

Adding Your Filer to the NTP Software File Auditor Policy Hierarchy

Next, you need to add your Filer to the collection of servers being monitored by NTP Software File Auditor.

1. Run NTP Software File Auditor Admin by clicking **Start** > **All Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor for NAS Admin**.
2. Right-click **My Site** and select **New** > **Filer**.
3. You will be prompted to enter a name. The name you enter here must match the name of your NetApp Filer.
4. Now that you have added your Filer to the collection of servers recognized by NTP Software File Auditor, right-click the Filer you just added and select **New** > **File Auditor Application**.
5. Next, you need to associate the policies you will create here with a Filer. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (**+**) adjacent to the name of the Windows-based server on which you installed NTP Software File Auditor.
6. Right-click **File Auditor** under that entry and select **Properties** to open the **NTP Software File Auditor Configuration** screen.
7. Click the **NAS Connector** tab.
8. Click the **Add** button.
9. Enter the name of your Filer/vFiler and click **OK**.
10. Click **OK** in the **NTP Software File Auditor Configuration** screen.

You are now ready to move on and create some File Auditor policies.

Copyright © 2012 by NTP Software®. All rights reserved.

Preparing the EMC Celerra

NOTE: Refer to this section only if you have one or more EMC Celerras attached to your environment. *If you do not have EMC Celerras, you should not apply the instructions specified in this section.*

Preparing EMC Celerra to be managed by File Auditor

Preparing File Auditor Windows Machine – Scenario A

This section describes how to prepare your EMC Celerra if you have either of the following environments:

- If you do not have an NTP Software Quota and File Sentinel (QFS) installation in your environment.
- If you have NTP Software and NTP Software Quota and File Sentinel (QFS) installed on the same machine.

If your QFS installation is older than version 7.1, you cannot manage the same EMC Celerra that QFS manages with File Auditor.

If your QFS installation is on a different machine, consult the section *Prepare EMC Celerra to be managed by File Auditor and QFS each installed on a separate machine*.

Configuring EMC Celerra Event Enabler (CEE)

Follow these steps to prepare the Windows machine to host NTP Software File Auditor:

1. Before installing NTP Software File Auditor, you have to make sure that Celerra Event Enabler (CEE) version 4.2.2 or later is appropriately installed and configured in your environment. Contact EMC for further information on this configuration.
2. NTP Software File Auditor requires the EMC Celerra to run DART version 5.6.36.2 or later. If your Celerra is not running version 5.6.36.2 or later, you must upgrade your operating system before you proceed. (Refer to your EMC documentation for instructions.)
3. After installing the Celerra Event Enabler on the NTP Software File Auditor machine, you need to specify the software with which the CEE will register. To do this, set **ntp** for the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CelerraEventEnabler\CEPP\CQM\Configuration\EndPoint

Copyright © 2012 by NTP Software®. All rights reserved.

Preparing the EMC Celerra for NTP Software File Auditor Management

For any Celerra that will be managed by NTP Software File Auditor, once the server is started and has mounted its root filesystem, go to the .etc directory and create the cepp.conf file (if it does not exist). You have to edit this file to include your CEPP pool description.

NOTE: The cepp.conf file must contain at least one line defining the pool of CEPP servers. If the line is too long, you can add \ at the end of each line:

pool name=<poolname> servers=<IP addr1>|<IP addr2>|... \
preevents=<event1>|<event2>|....\
postevents=<event3>|<event4>|.. \
posterrevents=<event5>|<event6>|... \
option=ignore or denied \
reqtimeout=<time out in ms> \ retrytimeout=<time out in ms>

Copyright © 2012 by NTP Software®. All rights reserved.

NOTES:

Each event can include one or more (or all) of the following events:

- OpenFileNoAccess
- OpenFileRead
- OpenFileWrite
- CreateFile
- CreateDir
- DeleteFile
- DeleteDir
- CloseModified
- CloseUnmodified
- RenameFile
- RenameDir
- SetAclFile
- SetAclDir

Postevents and posterrevents are not supported in NTP Software File Auditor. We recommend turning them off to improve performance. Dropping those two fields from the CEPP will stop the Celerra from generating events of those types.

At least one event, one pool, and one server per pool must be defined.

Recommended timeout values:

- The recommended value for *reqtimeout* is 5000.
- The recommended value for *retrytimeout* is 750.

Copyright © 2012 by NTP Software®. All rights reserved.

Apply the following steps to edit the cepp.conf file:

NOTE: Replace **server_2** with the name of the server you want to configure.

1. Log on to the Celerra control station as **su**.
    a. Type **mount server_2:/ /mnt2** to mount the root filesystem. (Create /mnt2 if it does not exist, and replace **server_2** with your server name if you are configuring a different server.)
    b. Type **cd /mnt2/.etc** and look for the file cepp.conf. Create the file if it does not exist.
    c. Use vi to edit the cepp.conf file. Edit the servers field to use the IP address of the machine running NTP Software File Auditor. The result should look something like this:

    pool name=cqm servers=10.30.3.57 preevents=* option=ignore reqtimeout=5000 retrytimeout=750
2. Type **.server_config server_2 -v "cepp stop"** and press **Enter**.
3. Type **.server_config server_2 -v "cepp start"** and press **Enter**.

These steps create the configuration that allows NTP Software File Auditor to register with and manage your Celerra. They must be completed before you attempt to configure NTP Software File Auditor.

Copyright © 2012 by NTP Software®. All rights reserved.

Adding a Celerra to the NTP Software File Auditor Policy Hierarchy

Next, you need to add your EMC Celerra to the collection of servers being monitored by NTP Software File Auditor:

1. Run NTP Software File Auditor Admin by clicking **Start** > **All Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor for NAS Admin**.
2. Right-click **My Site** and choose **New** > **Celerra**.
3. You will be prompted to enter a name. The name you enter here must match the name of your CIFS server.
4. Now that you have added your CIFS server to the collection of servers recognized by NTP Software File Auditor, right-click the CIFS server you just added and select **New** > **File Auditor Application**.
5. Next, you need to associate the policies you will create here with a CIFS server. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (**+**) adjacent to the name of the Windows-based server on which you installed NTP Software File Auditor.
6. Right-click **File Auditor** under that entry and select **Properties** to open the **NTP Software File Auditor Configuration** screen.
7. Click the **EMC Connector** tab.
8. Click the **Add** button.
9. Enter the name of your CIFS server the control station IP, user name, and password and then click **OK**.
10. Click **OK** in the **NTP Software File Auditor Configuration** screen.

You are now ready to move on and create some File Auditor policies.

Copyright © 2012 by NTP Software®. All rights reserved.

Preparing File Auditor Windows Machine – Scenario B

This section describes how to prepare your EMC Celerra If you have an installation of NTP Software Quota and File Sentinel (QFS) 7.1 or higher on a different machine and you want QFS to manage the same EMC Celerra that File Auditor will manage, perform the following steps.

NOTES:

If your QFS installation is older than version 7.1, you cannot manage the same EMC Celerra that QFS manages with File Auditor.

If QFS and File Auditor are both installed on the same machine consult the section *Prepare EMC Celerra to be managed by File Auditor*.

If you do not have QFS in your environment, consult the section *Prepare EMC Celerra to be managed by File Auditor*.

Configure EMC Celerra Event Enabler (CEE)

Follow these steps to prepare the Windows machine that hosts NTP Software QFS:

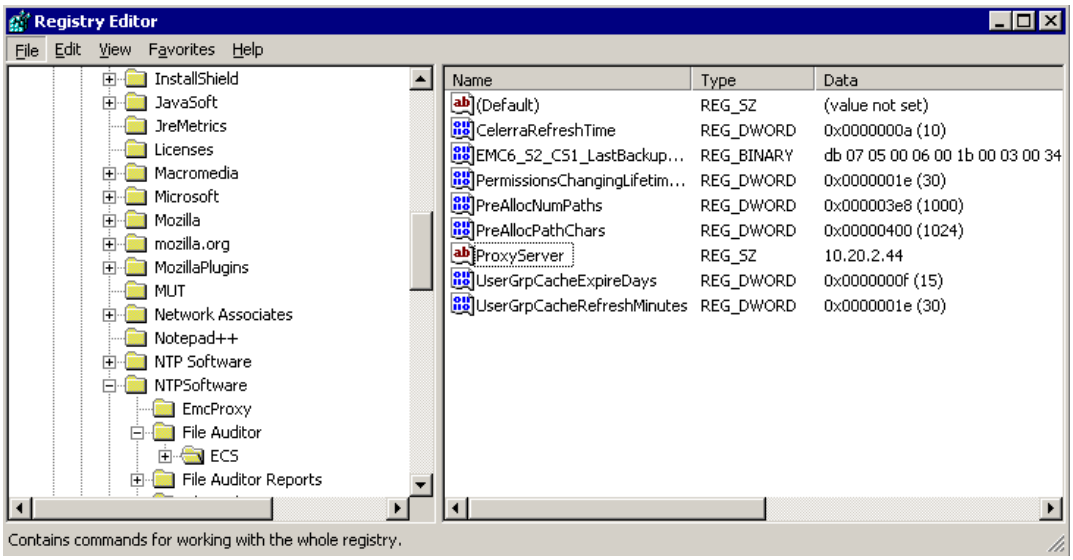
- Before installing NTP Software QFS, you have to make sure that Celerra Event Enabler (CEE) version 4.2.2 or later is appropriately installed and configured in your environment. Contact EMC for further information on this configuration.
- NTP Software File Auditor requires the EMC Celerra to run DART version 5.6.36.2 or later. If your Celerra is not running version 5.6.36.2 or later, you must upgrade your operating system before you proceed. (Refer to your EMC documentation for instructions.)
- After installing the Celerra Event Enabler on the NTP Software QFS machine, you need to specify the software with which the CEE will register. To do this, set **ntp** for the following key:

  HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CelerraEvent Enabler\CEPP\CQM\Configuration\EndPoint

- Make sure that the NTP Software EMC Proxy Service is started:
  a. Open the Windows Service Manager from Control Panel\Administrative tools\Services
  b. Look for NTP Software EMC Proxy Service entry, and make sure its status is **Started.**

Copyright © 2012 by NTP Software®. All rights reserved.

- On the NTP Software File Auditor machine, you need to specify the machine on which NTP Software QFS resides. To do this, perform the following steps:
    a. Go to the following key in the registry editor HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\File Auditor\ECS
    b. Create a string value called **ProxyServer** if it does not exist.
    c. Set the **ProxyServer** value to the machine IP or name of the NTP Software Quota and File Sentinel machine.
- On the NTP Software File Auditor machine, Make sure that the NTP Software EMC Proxy Service is disabled:
    a. Open the Windows Service Manager from Control Panel\Administrative tools\Services
    b. Look for NTP Software EMC Proxy Service entry; right click this entry and select **Stop.**
    c. Right click NTP Software EMC Proxy Service entry, and select **Properties**, then in the **General** tab, change **Startup type** to **Disabled**.



- On the NTP Software File Auditor machine, restart the NTP Software File Auditor EMC Connector Service.
    a. Open the Windows Service Manager from Control Panel\Administrative tools\Services
    b. Restart the NTP Software File Auditor EMC Connector Service**.**

Copyright © 2012 by NTP Software®. All rights reserved.

Preparing the EMC Celerra for NTP Software File Auditor Management

For any Celerra that will be managed by NTP Software File Auditor, once the server is started and has mounted its root filesystem, go to the .etc directory and create the cepp.conf file (if it does not exist). You have to edit this file to include your CEPP pool description.

NOTE: The cepp.conf file must contain at least one line defining the pool of CEPP servers. If the line is too long, you can add \ at the end of each line:

pool name=<poolname> servers=<IP addr1>|<IP addr2>|... \

preevents=<event1>|<event2>|....\

postevents=<event3>|<event4>|.. \

posterrevents=<event5>|<event6>|... \

option=ignore or denied \

reqtimeout=<time out in ms> \ retrytimeout=<time out in ms>

ADDITIONAL NOTES:

Each event can include one or more (or all) of the following events:

- OpenFileNoAccess
- OpenFileRead
- OpenFileWrite
- CreateFile
- CreateDir
- DeleteFile
- DeleteDir
- CloseModified
- CloseUnmodified
- RenameFile
- RenameDir
- SetAclFile
- SetAclDir

Postevents and posterrevents are not supported in NTP Software File Auditor. We recommend turning them off to improve performance. Dropping those two fields from the CEPP will stop the Celerra from generating events of those types.

At least one event, one pool, and one server per pool must be defined.

Copyright © 2012 by NTP Software®. All rights reserved.

Recommended timeout values:

- The recommended value for *reqtimeout* is 5000.
- The recommended value for *retrytimeout* is 750.

Apply the following steps to edit the cepp.conf file:

1. Log on to the Celerra control station as **su**.
    a. Type **mount server_2:/ /mnt2** to mount the root filesystem. (Create /mnt2 if it does not exist, and replace **server_2** with your server name if you are configuring a different server.)
    b. Type **cd /mnt2/.etc** and look for the file cepp.conf. Create the file if it does not exist.
    c. Use vi to edit the cepp.conf file. Edit the servers field to use the IP address of the machine running NTP Software File Auditor and the machine running NTP Software QFS. The result should look something like this:

    pool name=cqm servers=10.30.3.57|10.30.3.58 preevents=* option=ignore reqtimeout=5000 retrytimeout=750
2. Type **.server_config server_2 -v "cepp stop"** and press **Enter**.
3. Type **.server_config server_2 -v "cepp start"** and press **Enter**.

NOTE: Replace **server_2** with the name of the server you want to configure.

These steps create the configuration that allows NTP Software File Auditor to register with and manage your Celerra. They must be completed before you try to configure NTP Software File Auditor.

Copyright © 2012 by NTP Software®. All rights reserved.

Adding a Celerra to the NTP Software File Auditor Policy Hierarchy

Next, you need to add your EMC Celerra to the collection of servers being monitored by NTP Software File Auditor:

1. Run NTP Software File Auditor Admin by clicking **Start** > **All Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor for NAS Admin**.
2. Right-click **My Site** and choose **New** > **Celerra**.
3. You will be prompted to enter a name. The name you enter here must match the name of your CIFS server.
4. Now that you have added your CIFS server to the collection of servers recognized by NTP Software File Auditor, right-click the CIFS server you just added and select **New** > **File Auditor Application**.
5. Next, you need to associate the policies you will create here with a CIFS server. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (**+**) adjacent to the name of the Windows-based server on which you installed NTP Software File Auditor.
6. Right-click **File Auditor** under that entry and select **Properties** to open the **NTP Software File Auditor Configuration** screen.
7. Click the **EMC Connector** tab.
8. Click the **Add** button.
9. Enter the name of your CIFS server the control station IP, user name, and password and then click **OK**.
10. Click **OK** in the **NTP Software File Auditor Configuration** screen.

You are now ready to move on and create some File Auditor policies.

Copyright © 2012 NTP Software

Preparing the BlueArc Titan or Hitachi NAS

NOTE: Refer to this section only if you have BlueArc Titans or Hitachi Hitachi NASs attached to your environment. *If you do not have* BlueArc Titans or Hitachi Hitachi NASs, *you should not apply the instructions specified in this section.*

Preparing the BlueArc Titan/ Hitachi NAS for NTP Software File Auditor Management

To prepare the Titan/Hitachi NAS server, the following must be taken into consideration:

1. For each EVS (virtual server) managed by NTP Software File Auditor, at least one CIFS server name must be created and must join the same domain as the NTP Software File Auditor machine.
2. The logon account used to register with the Titan server (the account that will be assigned to the NTP Software File Auditor service) needs to be a member of the Titan server's local group **Backup Operators**, which can be added from the Titan Server command-line interface (CLI) using the following command:

   localgroup add "Backup Operators" <FQDomainName\AccountName>
3. The File-Filtering feature must be enabled. To enable it, use the following command:

   fsm set allow-ntp-file-filtering true

Copyright © 2012 NTP Software

Adding an EVS to the NTP Software File Auditor Policy Hierarchy

Next, you need to add your EVS to the collection of servers being managed by NTP Software File Auditor:

1. Run NTP Software File Auditor Admin by clicking **Start** > **All Programs** > **NTP Software File Auditor for NAS** > **NTP Software File Auditor for NAS Admin**.
2. Right-click **My Site** and choose **New** > **EVS**.
3. You will be prompted to enter a name. The name you enter here must match the name of your EVS.
4. Now that you have added your EVS to the collection of servers recognized by NTP Software File Auditor, right-click the EVS you just added and select **New** > **File Auditor Application**.
5. Next, you need to associate the policies you will create here with an EVS In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (**+**) adjacent to the name of the Windows-based server on which you installed NTP Software File Auditor.
6. Right-click **File Auditor** under that entry and select **Properties** to open the **NTP Software File Auditor Configuration** screen.
7. Click the **BlueArc/Hitachi Connector** tab.
8. Click the **Add** button.
9. Enter the name of your EVS.
10. Click **OK**.
11. Click **OK** in the **NTP Software File Auditor Configuration** screen.

You are now ready to move on and create some File Auditor policies.

Copyright © 2012 NTP Software

About NTP Software

NTP Software puts users in charge of their file data and is the only company providing file data management solutions that deliver all of the enterprise-class features needed to understand, manage, monitor, and secure file data completely. NTP Software is a global leader and has been chosen by the majority of Fortune 1000 companies and thousands of customers in private and public sectors for providing leadership through superior solutions, professional services, experience, and trusted advice. NTP Software delivers a single solution across the entire data storage environment, from individual files and users to an entire global enterprise across thousands of systems and sites. NTP Software reduces the cost and complexity associated with the exponential growth of file data and is located on the web at www.ntpsoftware.com.

NTP Software Professional Services

NTP Software's Professional Services offers consulting, training, and design services to help customers with their storage management challenges. We have helped hundreds of customers to implement cost-effective solutions for managing their storage environments. Our services range from a simple assessment to in-depth financial analyses.

For further assistance in creating the most cost-effective Storage Management Infrastructure, please contact your NTP Software Representative at 800-266-2755 or 603-622-4400.

Copyright © 2012 NTP Software

The information contained in this document is believed to be accurate as of the date of publication. Because NTP Software must constantly respond to changing market conditions, what is here should not be interpreted as a commitment on the part of NTP Software, and NTP Software cannot guarantee the accuracy of any information presented after the date of publication.

This user manual is for informational purposes only. NTP SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

NTP Software and other marks are either registered trademarks or trademarks of NTP Software in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

NTP Software products and technologies described in this document may be protected by United States and/or international patents.

NTP Software

20A Northwest Blvd., #136

Nashua, NH 03063

Toll Free: 800-226-2755

International: 1-603-622-4400

Web Site: http://www.ntpsoftware.com

Copyright © 2012 NTP Software. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. Doc# 4372EF